Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Base size, metric dimension and other invariants of groups and graphs

Robert F. Bailey and Peter J. Cameron

Abstract

The base size of a permutation group, and the metric dimension of a graph, are two of a number of related parameters of groups, graphs, coherent configurations and association schemes. They have been repeatedly re-defined with different terminology in various different areas, including computational group theory and the graph isomorphism problem. We survey results on these parameters in their many incarnations, and propose a consistent terminology for them. We also present some new results, including on the base sizes of wreath products in the product action, and on the metric dimension of Johnson and Kneser graphs.

1. *Introduction*

The base size of a permutation group is the smallest number of points whose stabiliser is the identity. The metric dimension of a graph is the smallest number of vertices such that all vertices are uniquely determined by their distances to the chosen vertices. The two parameters are related by a straightforward inequality: the metric dimension of a graph gives an upper bound on the base size of its automorphism group. Neither parameter is new: base size has a history dating back around 40 years, while metric dimension dates back over 30 years. Both parameters have been heavily studied, by a variety of authors, especially in the last decade. Furthermore, as we shall see, both parameters keep being rediscovered, or reinvented, in different guises.

The purpose of this paper is not to be a complete survey of either base size or of metric dimension, but rather to describe those cases where relationship between the two is particularly interesting. Primarily, this is when the permutation group is the automorphism group of a graph with a considerable amount of symmetry or regularity. As well as surveying existing results, we also introduce some new material: the main new results are Theorem 2.13 on the base sizes of wreath products in the product action, and Theorem 3.32 on the metric dimension of Johnson and Kneser graphs. Other results which are not new but which we have re-interpreted include Theorems 2.9 and 2.10 on the distinguishing numbers of finite primitive groups, and results due to Babai that give bounds on the metric dimension of distance-regular and strongly-regular graphs (Theorems 3.15, 3.22 and 3.31). In Theorem 2.22, we give a previously unpublished result of Maund on the base size of the symmetric group acting on subsets.

As this paper is concerned with both groups and graphs, we need to decide upon our notation carefully. Throughout, G will denote a permutation group, which will be assumed to be finite unless otherwise stated, acting upon a set Ω. The *degree* of G is the size of Ω. Graphs will be denoted by Γ, with vertex set V and edge set E; the group of automorphisms of Γ will be denoted by $\mathrm{Aut}(\Gamma)$.

2000 *Mathematics Subject Classification* 05C25 (primary), 05C12, 05C78, 05E30, 20B05 (secondary).

2. *Bases and base sizes*

2.1. *Background*

The following definition is a fundamental one in permutation group theory.

DEFINITION 2.1. A *base* for a permutation group G acting faithfully on a finite set Ω is a subset $B \subseteq \Omega$ chosen so that its pointwise stabiliser in G is trivial.

Bases were originally introduced in the 1960s by Sims [**89**], in the context of computational group theory. Indeed, many algorithms for computing with finite permutation groups use bases (see Seress [**88**] for examples). However, the concept can be traced back to the work of Bochert in the 19th century [**16**]. Bases have the property that the action of an element $g \in G$ is uniquely determined by its action on a base, so in a reasonable sense, bases generalise the notion of bases in vector spaces. (Indeed, a basis for $\mathbb{F}_q^n$ is a base for the action of $\mathrm{GL}(n, q)$ on the non-zero vectors.)

A base is *minimal* if no proper subset of it is a base. In computational group theory, bases are usually treated as ordered sequences of points $[x_1, \ldots, x_b]$. This is because the ordering defines a chain of subgroups, the *stabiliser chain*,

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_b = 1,$$

where G_i denotes the pointwise stabiliser of the subsequence $[x_1, \ldots, x_i]$. If all the inclusions in the stabiliser chain are strict, the base is called *irredundant*. We note that being irredundant is a property of the ordering of the base: reordering may introduce redundancy. For example, the group $G = \langle (1,3)(2,6)(5,7)(4,8), (2,4)(3,6,7,8) \rangle$ has both $[1, 2, 3]$ and $[1, 3]$ as irredundant bases. Clearly, however, any minimal base is irredundant in any ordering.

The *base size* of a group G in its action on Ω is the cardinality of the smallest base for G in this action; we denote this by $b(G)$. Some straightforward examples are given below.

EXAMPLE 2.2. In their natural actions on n points, the symmetric group S_n has base size $n - 1$, and the alternating group A_n has base size $n - 2$.

EXAMPLE 2.3. More generally, for a sharply k-transitive group G (i.e. for any two ordered k-tuples of distinct points, there exists a unique $g \in G$ mapping the first to the second) has base size k (since the stabiliser of any k-tuple is trivial, by definition).

EXAMPLE 2.4. The general linear group $\mathrm{GL}(n, q)$ acting on the non-zero vectors of $\mathbb{F}_q^n$ has base size n.

As well as having practical implications for computational purposes, determining base sizes is of much theoretical interest, especially because of the following inequality. For any permutation group G of degree n, we have

$$2^{b(G)} \leq |G| \leq n^{b(G)}$$

which follows from considering the maximum and minimum possible indices in the stabiliser chain. Using this, one can obtain bounds on the orders of groups in a given class by bounding the sizes of bases for such groups.

In recent years, a considerable body of work has been developed determining the base sizes of groups, particularly primitive actions of almost simple groups. This study was begun by Cameron and Kantor [**36**] in 1993, and has been continued by various authors including Liebeck and Shalev [**25**, **75**, **77**, **78**], James [**68**, **69**], and by Burness and various coauthors [**23**, **24**, **25**, **26**]; broadly speaking, the purpose of this work has been to show that if a primitive action of an almost simple group is "non-standard" (for example, not on subspaces of the natural module of a classical group), then the base size is at most 7. In many cases, it is actually a constant less than 7, with the extreme case being the 24-point action of the Mathieu group M_{24}.

Also in a 1993 paper, Pyber [**82**] conjectured that there is an absolute constant c such that for a primitive permutation group G of degree n,

$$b(G) \leq c \cdot \frac{\log |G|}{\log n}.$$

Progress towards this conjecture has been made by Gluck and various coauthors [**59**, **60**], by Liebeck and Shalev [**76**], and in the (unpublished) Ph.D. thesis of Benbenishty [**13**]; see [**77**] for further details. Another interesting result is due to Seress, who showed in a 1996 paper [**86**] that a primitive, soluble permutation group has a base of size at most 5. Algorithmically, determining the base size of a permutation group is an NP-hard problem: this was shown by Blaha [**15**] in 1992.

Given that bases are a natural concept, it is perhaps not surprising that the notion has arisen independently on a number of occasions. This is especially true in the context of automorphism groups of graphs, where at least three different pieces of terminology have been used, and in each case the parameter $b(G)$ is treated as a property of the graph rather than the automorphism group.

Let $\Gamma = (V, E)$ denote a finite graph, and suppose that $G = \mathrm{Aut}(\Gamma)$. Erwin and Harary [**53**] used the term *fixing set* to mean a base for $\mathrm{Aut}(\Gamma)$, and call the base size the *fixing number* of Γ. In a similar manner, Boutin [**19**] used the term *determining set* to mean a base for $\mathrm{Aut}(\Gamma)$, and calls the base size of $\mathrm{Aut}(\Gamma)$ the *determining number* of Γ. Also, Fijavž and Mohar [**55**] call the base size of $\mathrm{Aut}(\Gamma)$ the *rigidity index* of Γ.

Not surprisingly, these reinventions have led to duplication of results in the literature. Also, many results which have been published in terms of graphs are really statements about permutation groups, and which are of interest from a purely group-theoretical point of view. The main aim of this section is to discuss some of these and put them into this context. Before doing so, we will introduce another, related, concept: the distinguishing number.

2.2. *Distinguishing number*

The *distinguishing number* of a permutation group G on Ω is defined to be the smallest number of parts in a partition of Ω with the property that only the identity fixes every part. Such a partition is called a *distinguishing partition*. While distinguishing partitions are not used widely in algorithms in computational group theory (in the way that bases are), the two concepts are related. For example, in [**86**], Seress showed that the distinguishing number of soluble permutation groups is at most 5, on the way to his result on the base sizes of primitive soluble groups. Also, in subsection 2.3 below, we use it in describing the base sizes of wreath products in the product action.

The term 'distinguishing number' arose in the graph-theoretic literature, where it was introduced in 1996 by Albertson and Collins [**2**] and has spawned a considerable number of papers by several authors. In this setting, it is customary to speak of a distinguishing partition or the distinguishing number of a graph to mean the corresponding objects for its automorphism group. The partition is commonly regarded as a labelling or colouring of the vertex set. This

colouring is not necessarily a proper graph colouring (where adjacent vertices have different colours), but this extra assumption has been considered by Collins and Trenk [**41**]; the number of colours needed is referred to as the *distinguishing chromatic number* of the graph.

We denote the distinguishing number of G by $D(G)$. Distinguishing number and base size are related by the inequality $D(G) \leq b(G) + 1$: given a minimum base B, we obtain a distinguishing partition by giving each point in B a different colour, and colouring all of $\Omega \setminus B$ with another colour. Given that "most" primitive groups are believed to have small base size, it should follow that "most" will have small distinguishing number. In what follows, we shall see that this is the case.

Some elementary properties of the distinguishing number are summarised in the next two results.

PROPOSITION 2.5. *A permutation group has distinguishing number* 1 *if and only if it is the trivial group.*

PROPOSITION 2.6. *The distinguishing numbers of the symmetric and alternating groups of degree n are n and $n-1$ respectively.*

In the case where G has distinguishing number 2, we also have the following characterisation.

PROPOSITION 2.7. *Let G be a permutation group acting on a finite set Ω. Then the following are equivalent:*

(i) *G has distinguishing number 2;*
(ii) *There is a subset of Ω whose setwise stabiliser in G is the identity;*
(iii) *G has a regular orbit on the power set of Ω.*

For example, let G be the symmetric group of degree n, acting on the set Ω of 2-element subsets of $\{1, \ldots, n\}$. A subset of Ω is the edge set of a graph, and its setwise stabiliser is the automorphism group of the graph. For $n \geq 6$, there is a graph with trivial automorphism group, so the distinguishing number of G is 2. Indeed, as $n \to \infty$, the proportion of graphs with trivial automorphism group tends to 1.

This pattern holds more generally. The following result is proved in two papers from the 1980s [**31**, **38**], where the problem was formulated in terms of regular orbits on the power set.

PROPOSITION 2.8. *Let G be a primitive permutation group of degreee n, which is not the symmetric or alternating group or one of a finite list of other groups. Then the distinguishing number of G is* 2*. Indeed, the proportion of subsets which have trivial stabiliser in a primitive group of degree n not containing the alternating group tends to* 1 *as $n \to \infty$.*

The exceptions in Proposition 2.8 were determined by Seress in 1997 ([**87**], Theorem 2).

THEOREM 2.9 (Seress [**87**]). *There are 43 groups with distinguishing number $D > 2$, of degrees $5 \leq n \leq 17$, $21 \leq n \leq 24$ and $n = 32$.*

As lemmas on the way to his main result, Seress also obtains results which have since been obtained independently in the language of distinguishing numbers of graphs. His Lemma 9

shows that the distinguishing number of the Kneser graph $K(n,k)$ (which we will see later in the paper in subsections 2.5 and 3.8) is 2 unless $n = 5$ and $k = 2$; this is the main result of Albertson and Boutin [**1**]. Also, Seress' Lemma 4 shows that $S_m \wr S_d$, acting in the product action (defined below), has distinguishing number 2 when $m \geq 5$ and $d \geq 2$, and Corollary 5 shows that this is true in general for wreath products in the product action. This implies the main result of Imrich and Klavžar [**66**] on distinguishing numbers of Cartesian powers of graphs (although Imrich and Klavžar also show what happens for $m \leq 4$).

In 2000, Dolfi [**45**] improved on Seress' results, by counting the number of regular orbits on the set of ordered partitions of Ω into a fixed number of parts. In particular, his Lemma 1 contains the following result, which we have translated into the language of distinguishing numbers.

THEOREM 2.10 (Dolfi [**45**]). *Of the 43 groups listed by Seress (cf. Theorem 2.9), 38 have distinguishing number 3 and five have distinguishing number 4. The five exceptions have degrees 6, 7, 8, 11 and 12.*

Thus the distinguishing numbers of all primitive groups are known. The results in Dolfi's paper also bound the distinguishing numbers of a large class of imprimitive and intransitive groups, namely those for which no primitive constituent of degree at least 5 contains the alternating group.

Finally, we note that almost 20 years before the paper of Albertson and Collins, Babai [**3**] showed that the distinguishing number of a regular infinite tree, even one with infinite valency, is 2.

2.3. *Direct and wreath products*

Let H and K be permutation groups on disjoint sets X and Y respectively. There are two standard products of H and K, the direct and wreath products, and each of these has two natural actions. In this subsection, we discuss the base sizes of each of these products.

The two actions of the direct product $H \times K$ are on $X \cup Y$ and on $X \times Y$. In the former case, it is straightforward to see that $b(H \times K) = b(H) + b(K)$. In the latter case, known as the *product action*, we have the following.

PROPOSITION 2.11. *Let $H \times K$ act in its product action on $X \times Y$. Then $b(H \times K) = \max\{b(H), b(K)\}$.*

Proof. Suppose $\{(x_1, y_1), \ldots, (x_b, y_b)\}$ is a base for $H \times K$. Then $\{x_1, \ldots, x_b\}$ must be a base for H and $\{y_1, \ldots, y_b\}$ must be a base for K. Hence $b \geq \max\{b(H), b(K)\}$, and the result follows. □

Note that simple induction arguments give formulas for the base sizes of direct products of arbitrarily many factors in each action.

The *wreath product* $H \wr K$ is the semidirect product $N \rtimes K$, where

$$N = \prod_{\delta \in Y} H_\delta$$

is the direct product of $|Y|$ copies of H (indexed by Y), and K acts on N by permuting the factors in the same way as it permutes elements of Y. There are two natural actions of the wreath product:

(i) The *imprimitive action* on $X \times Y$: for each $\delta \in Y$, the copy H_δ of H in N acts on the corresponding copy

$$X_\delta = \{(\gamma, \delta) : \gamma \in X\}$$

of X, while K permutes the copies of X according to its given action on Y.

(ii) The *product action* (also known as the *power action*) on X^Y: think of X^Y either as the Cartesian product of $|Y|$ copies of X, or as the set of all functions $f : Y \to X$. This time N acts coordinatewise, so that the factor H_δ acts on the values $f(\delta)$ of a function f, while the group K acts by permuting the arguments of the function, by $f^k(\delta) = f(\delta^{k^{-1}})$.

The base size for the imprimitive action is easy to compute:

PROPOSITION 2.12. *Let H and K act on X and Y, and let $G = H \wr K$ have its imprimitive action. Then*

$$b(H \wr K) = |Y| \cdot b(H).$$

Proof. For each $\delta \in Y$, if we have fewer than $b(H)$ points of X_δ in, then they are fixed by a non-identity element of H_δ; on the other hand, it is clear that if we choose a base in each copy of X then we obtain a base for G. □

To find the base size for the wreath product $H \wr K$ in the product action (in terms of $b(H)$ and $b(K)$) is more complicated. However, the following theorem, in principle, gives us what we desire. For this subsection only, we define an *ordered multi-base* to be a sequence of points (with repetitions allowed) whose stabiliser is the identity.

THEOREM 2.13. *Let H and K be permutation groups. Then $H \wr K$ (in the product action) has a base of size t if and only if the number of orbits of H on ordered multi-bases of length t is not less than the distinguishing number of K.*

Proof. Throughout, we suppose H and K act on sets X and Y respectively, where $|X| = m$.

Suppose first that the inequality holds. Let $D = D(K)$, and choose D multi-bases for H belonging to distinct orbits, say $B_1, \ldots, B_D$. Choose also a distinguishing partition for K. Now define functions $f_i : Y \to X$ for $i = 1, \ldots, t$ (where X and Y are the permutation domains for H and K) as follows: construct an $m \times t$ array of points of X, where the ith row is B_s if i lies in the sth part of the distinguishing partition; then let f_j be the jth column of the array.

We claim that these functions form a base for $H \wr K$. Suppose that $g \in H \wr K$ is an element fixing all of them. Because bases corresponding to points in different parts lie in different orbits, g must fix the distinguishing partition part-wise, and hence g projects onto the identity in K, that is, $g \in N$. But the values of the functions on any coordinate form a base for H; so $g = 1$, as required.

Conversely, suppose that the inequality fails. Choose any t functions. If their values on the ith coordinate do not form a multi-base for H, then some non-identity element of N fixes all of them; so suppose otherwise. Write the functions as columns of an array whose rows are now known to be multi-bases for H. Partition Y according to the H-orbit containing the corresponding multi-base. By hypothesis, the number of parts of this partition is strictly smaller than the distinguishing number of K; so there is a non-identity element $k \in K$ fixing this partition part-wise.

For any $i \in \{1, \ldots, t\}$, the multi-bases formed by columns i and i^k belong to the same orbit of H, so we may postmultiply by an element of H in the i^k coordinate to ensure that they are

actually equal. Then the resulting modified element fixes all the functions, so that they do not form a base for $H \wr K$. □

The difficulty in applying this theorem is that it involves finding the number of H-orbits on ordered multi-bases of size t. We suspect that there is an inclusion-exclusion formula for this. But we can certainly bound it below by $s \cdot m^{t-b}$, where m is the degree of H, $b = b(H)$ and s is the number of H-orbits on ordered bases of minimum size; for this is the number of orbits on t-tuples whose first b entries form a base. This shows the following:

COROLLARY 2.14. *Whenever $D = D(K) \geq s$, we have*

$$b(H \wr K) \leq b(H) + \lceil \log_m(D/s) \rceil.$$

Proof. If N_t denotes the number of H-orbits on ordered multi-bases of size t, then

$$\begin{aligned} b(H \wr K) &= \min\{t : N_t \geq D\} \\ &\leq \min\{t : sm^{t-b} \geq D\} \\ &= b + \lceil \log_m(D/s) \rceil. \end{aligned}$$

□

The case where $s = 1$ is when H is *base-transitive*. Such groups were classified in the late 1980s by Maund [**80**] and Zil'ber [**97**]; a statement of the classification is given in Section 2 of [**8**]. In this situation, we have another corollary.

COROLLARY 2.15. *Suppose H is base-transitive of degree m, and that K is a non-trivial permutation group with $D(K) \leq m$. Then, for $H \wr K$ acting in the product action, $b(H \wr K) = b(H) + 1$.*

Proof. Since $2 \leq D \leq m$, it follows that $0 < \log_m(D) \leq 1$, and so the previous corollary gives us an upper bound of $b(H \wr K) \leq b(H) + 1$.

To obtain a lower bound, we note since the subgroup $N = H \times H \times \cdots \times H$ is a direct product in the product action, the remark after Proposition 2.11 implies $b(N) = b(H)$, and clearly $b(N) \leq b(H \wr K)$. So we must show that no minimal base for N is a base for $H \wr K$.

Since H is base-transitive, we can consider, without loss of generality, a base for N of the form B^Y, where B is a minimal base for H. But clearly K permutes the copies of B in the same way it permutes the copies of X, so B^Y cannot be a base for $H \wr K$.

Thus $b(H) < b(H \wr K) \leq b(H) + 1$, and the result follows. □

As an example of the use of this corollary, we give a result mentioned by Babai [**5**].

EXAMPLE 2.16. For $m \geq 2$, the base size of $G = S_m \wr S_2$, acting in the product action on $\{1, \ldots, m\}^2$, is $b(G) = m$: since $D(S_2) = 2$, S_m is base-transitive and $b(S_m) = m - 1$, we can immediately apply Corollary 2.15 and obtain $b(G) = (m-1) + 1 = m$. An example of a minimal base is

$$\{(1,1), (2,2), \ldots, (m-1, m-1), (1,2)\}.$$

In fact, the same argument shows that whenever $d \leq m$ we have $b(S_m \wr S_d) = m$.

The requirement in Corollary 2.15 that H is base-transitive cannot be weakened. For instance, if the number s of H-orbits on ordered bases of minimum size is at least $D(K)$, then Corollary 2.14 implies that $b(H \wr K) = b(H)$. An example is the group $D_{10} \wr S_2$, which has base size 2 since $s = D = 2$.

We conclude this subsection with another application of Theorem 2.13, to wreath products of symmetric groups. Recall that the *Stirling number of the second kind*, denoted $S(n, k)$, is the number of partitions of an n-set into k non-empty parts (see [**32**], Section 5.3).

PROPOSITION 2.17. *The base size of $S_m \wr S_d$, acting in the product action, is the smallest integer t for which $S(t, m) + S(t, m-1) \geq d$.*

Proof. By Theorem 2.13, $b(S_m \wr S_d) \leq t$ if and only if the number of orbits of S_m on ordered multi-bases of length t is at least $D(S_d) = d$. Now, a t-tuple is a multi-base for S_m if and only if its image has size m or $m-1$, and the number of such t-tuples is $m!S(t, m) + m(m-1)!S(t, m-1)$. Dividing by $m!$, we obtain $S(t, m) + S(t, m-1)$ orbits on bases. Thus $b(S_m \wr S_d)$ is the least t for which $S(t, m) + S(t, m-1) \geq d$. □

It would perhaps be desirable to obtain an asymptotic result for this in terms of m and d. However, in particular cases, for fixed, small values of m, we can give precise answers. We give the results for $m = 2$ and $m = 3$ below.

COROLLARY 2.18. *In the product action, the base size of $S_2 \wr S_d$ is $1 + \lceil \log_2 d \rceil$, and the base size of $S_3 \wr S_d$ is $1 + \lceil \log_3(2d+1) \rceil$.*

Proof. We apply Proposition 2.17 with $m = 2$ and with $m = 3$. Now, when $m = 2$, none of the 2^t sequences over $\{1, 2\}$ are fixed by S_2, and there are 2^{t-1} orbits (note that $S(t, 2) + S(t, 1) = 2^{t-1}$). So the base size $b(S_2 \wr S_d)$ is t as long as $2^{t-1} \geq d$, that is, $t \geq 1 + \log_2 d$. Hence we have $b(S_2 \wr S_d) = 1 + \lceil \log_2 d \rceil$.

In the case $m = 3$, S_3 has $3^t - 3$ bases of length t (all except constant sequences), falling into $(3^t - 3)/6 = (3^{t-1} - 1)/2$ orbits (note that $S(t, 3) + S(t, 2) = (3^{t-1} - 1)/2$). So the base size $b(S_3 \wr S_d)$ is t as long as $(3^{t-1} - 1)/2 \geq d$, that is, $t \geq 1 + \log_3(2d+1)$. In other words, we have $b(S_3 \wr S_d) = 1 + \lceil \log_3(2d+1) \rceil$. □

In the next subsection, we will see how direct and wreath products in the product action arise naturally as automorphism groups of graphs.

2.4. *Cartesian products and Hamming graphs*

The following operation is well-known in graph theory as a means of "multiplying" graphs.

DEFINITION 2.19. Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ be graphs. Then the *Cartesian product* $\Gamma_1 \,\square\, \Gamma_2$ is the graph with vertex set $V_1 \times V_2$, and where $(v_1, v_2) \sim (w_1, w_2)$ if either $v_1 = w_1$ and $v_2 w_2 \in E_2$ or $v_2 = w_2$ and $v_1 w_1 \in E_1$.

Furthermore, we denote $\Gamma \,\square\, \Gamma \,\square\, \cdots \,\square\, \Gamma$ (with k factors) by Γ^k. A graph is *prime* with respect to the Cartesian product if it cannot be expressed as the Cartesian product of smaller graphs. Cartesian products were introduced by Sabidussi in 1960 [**84**], where he proved the following.

THEOREM 2.20 (Sabidussi [**84**]). *Let Γ be a finite, connected graph. Then:*

(i) *There is a unique set of prime graphs $\Gamma_1, \ldots, \Gamma_k$ such that*

$$\Gamma = \Gamma_1^{n_1} \,\square\, \cdots \,\square\, \Gamma_k^{n_k}$$

for some integers $n_1, \ldots, n_k$;

(ii) *The automorphism group of Γ is of the form*

$$\mathrm{Aut}(\Gamma) = (G_1 \wr S_{n_1}) \times \cdots \times (G_k \wr S_{n_k})$$

where $G_i = \mathrm{Aut}(\Gamma_i)$, and all direct and wreath products are in their product actions.

The first part was also proved independently by Vizing [**94**]. Both parts are discussed by Imrich and Klavžar [**65**], in Sections 4.1 and 4.2 respectively, but the terminology of wreath products is used neither there nor in Sabidussi's original paper. Note that in the case of the Cartesian product of two relatively prime graphs Γ_1 and Γ_2, we have $\mathrm{Aut}(\Gamma_1 \,\square\, \Gamma_2) = \mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2)$ (in the product action), while in the case of Cartesian powers of a given prime graph Γ, we have

$$\mathrm{Aut}(\Gamma^k) = \mathrm{Aut}(\Gamma) \wr S_k.$$

Consequently results about direct and wreath products in their product actions give us corollaries about automorphism groups of Cartesian products. Also, as we shall see, many results stated in terms of such graphs are really special cases of these group-theoretical results.

The *Hamming graph* $H(d, m)$ is defined as follows. Its vertex set is the set of all words of length d over an alphabet of size m, and two vertices are adjacent if and only if the words differ in precisely one entry (i.e. their Hamming distance is 1). It follows that the distance between two vertices is the Hamming distance between the two corresponding words.

Two straightforward examples of Hamming graphs are $H(d, 2)$, which is the d-dimensional hypercube, and $H(2, m)$, which is the line graph of $K_{m,m}$, and is also known as the *square lattice graph* (see [**37**], Example 2.8) or *rook's graph*. $H(3, 2)$ and $H(2, 3)$ are shown in Figure 1 below.

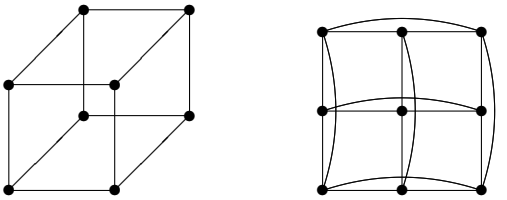


FIGURE 1. *The Hamming graphs $H(3, 2)$ (left) and $H(2, 3)$ (right).*

An alternative way to describe the Hamming graph is as the Cartesian product of d copies of the complete graph on m vertices, K_m^d. We note that some authors (such as Imrich and Klavžar [**65**]) use the term Hamming graph to describe a Cartesian product of complete graphs of different sizes. From Sabidussi's Theorem (Theorem 2.20), it follows that the automorphism group of $H(d, m)$ is the wreath product $S_m \wr S_d$, acting in the product action (although this can also be seen directly).

In the previous subsection, we obtained results on the base sizes of direct and wreath products in the product action. We conclude this subsection by showing how these generalise results in the graph theory literature, which are expressed in terms of Cartesian products of graphs. For instance, Theorem 1 of Boutin [**20**] and Theorem 4 of Cáceres *et al.* [**28**] both give restatements of Proposition 2.11 in the case of Cartesian products.

A deeper result is Theorem 5 of Boutin [**20**]. This states that, for a given integer k, the maximum d for which the base size of $\mathrm{Aut}(H(d,m))$ is k is equal to the number of equivalence classes of $m \times k$ *covering matrices*. A covering matrix is defined to be a 01-matrix with distinct rows and a single 0 in each column; two such matrices are equivalent if there is a permutation of the rows taking one to the other. However, if we transpose such a matrix and interchange the rôles of 0 and 1, we obtain precisely the incidence matrix of a partition of the set $\{1,\ldots,k\}$ into either m or $m-1$ parts (an all-zero column would correspond to an empty part). Thus the number of equivalence classes is the number of such set partitions, which is given by the sum of the Stirling numbers $S(k,m)$ and $S(k,m-1)$. Consequently, we recover the result of Proposition 2.17.

Our use of this result in Corollary 2.18 gives two more of Boutin's results in [**20**]: her Theorem 3, expressed as the determining number of the hypercube, is that $b(S_2 \wr S_d) = 1 + \lceil \log_2 d \rceil$, while her Corollary 6.1, expressed as the determining number of K_3^d, is that $b(S_3 \wr S_d) = 1 + \lceil \log_3(2d+1) \rceil$.

2.5. *The symmetric group, Johnson and Kneser graphs, and the greedy algorithm*

Consider the symmetric group S_n. One of the natural actions of S_n is on the set $\Omega = \binom{\{1,\ldots,n\}}{k}$ of all k-subsets of $\{1,\ldots,n\}$: for $2 \le k < n/2$, this action is primitive. Two well-known families of graphs have S_n, acting in this way, as their automorphism group.

The *Johnson graph* $J(n,k)$ has vertex set $\Omega = \binom{\{1,\ldots,n\}}{k}$, and two subsets X and Y are adjacent if and only if $|X \cap Y| = k-1$. The *Kneser graph* $K(n,k)$ is defined similarly: it also has vertex set Ω, and two vertices are adjacent if and only if the corresponding k-subsets are disjoint. In the case $k=2$, we can think of the 2-subsets as edges of the complete graph K_n: the Johnson graph $J(n,2)$ is its line graph, and the Kneser graph $K(n,2)$ is its complement.

EXAMPLE 2.21. The Kneser graph $K(5,2)$ is the well-known *Petersen graph*, as shown in Figure 2. The vertex labels are the corresponding 2-subsets of $\{1,\ldots,5\}$.

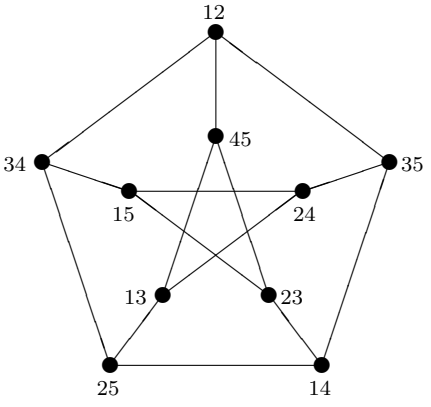


FIGURE 2. *The Petersen graph.*

Base sizes for the action of S_n on k-subsets were first studied in the (unpublished) 1989 D.Phil. thesis of Maund [**80**]. We summarise Maund's results below, which include a characterisation of bases for this action.

THEOREM 2.22 (Maund [**80**]). *Let G denote the action of S_n on k-subsets of $\{1,\dots,n\}$. Then:*

(i) *A family of k-subsets $\mathcal{B} = \{X_1,\dots,X_t\}$ is a base for G if and only if, for all $x, y \in \{1,\dots,n\}$ with $x \neq y$, there is some $X_i \in \mathcal{B}$ such that $|X_i \cap \{x,y\}| = 1$.*
(ii) *$b(G) \geq \lceil 2(n-1)/(k+1) \rceil$.*
(iii) *If $k(k+1)/2$ divides $n-1$, then $b(G) = 2(n-1)/(k+1)$.*

EXAMPLE 2.23. Suppose $k(k+1)/2$ divides n, for $k = 2, 3, 4$. In that case, we can "cover" the n points with disjoint copies of the configurations shown in Figure 3 to obtain minimum bases for the action of S_m on k-subsets.

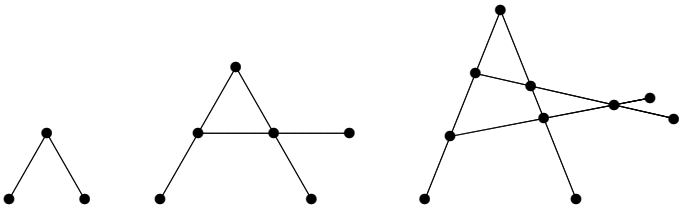


FIGURE 3. *Some minimum bases for S_n acting on k-subsets, where $k(k+1)/2 \mid n$, and $k = 2, 3, 4$.*

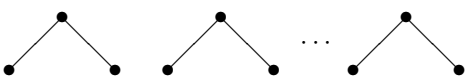
Maund also considers the case when $k(k+1)/2$ does not divide $n-1$ in detail, and the results are rather more complicated.

In the special case of $k = 2$, we can be more specific. Thinking of the 2-subsets as the edges of K_n, Maund's criterion translates as follows: a base for S_n acting on the edges of K_n consists of the edges of a spanning subgraph with no isolated edges and at most one isolated vertex. With that in mind, the next result is straightforward.

PROPOSITION 2.24. *Let G be the symmetric group S_n in its action on 2-subsets. Then $b(G)$ is dependent on congruence classes modulo 3:*

(i) *For $n \equiv 0 \pmod 3$, $b(G) = \frac{2}{3}n$;*
(ii) *For $n \equiv 1 \pmod 3$, $b(G) = \frac{2}{3}(n-1)$;*
(iii) *For $n \equiv 2 \pmod 3$, $b(G) = \frac{2}{3}(n-2)+1$.*

Proof. To see this, in the case where $n \equiv 0 \pmod 3$, we notice that a spanning subgraph of the following form is a base for G.



Furthermore, no graph with fewer edges will satisfy the criteria. When $n \equiv 1 \pmod 3$, we add an extra isolated vertex; when $n \equiv 2 \pmod 3$, we add two extra vertices: one joined to an incident pair somehow, the other remaining isolated. □

The equivalent problem of finding the determining numbers of Kneser graphs has been considered more recently, starting in the 2006 paper of Boutin [**19**], and continued in the recent work of Cáceres *et al.* [**27**]. Their methods and results are very similar to Maund's, although

were obtained independently, and are expressed in the language of graphs and hypergraphs. Their main theorem implies parts (ii) and (iii) of Maund's Theorem 2.22.

THEOREM 2.25 (Cáceres *et al.* [**27**]). *Let G denote the action of S_n on k-subsets of $\{1, \ldots, n\}$. Then:*

(i) *If b is a positive integer satisfying $b > 2$ and $k \leq b$, and where $n = \lfloor \frac{d(k+1)}{2} \rfloor + 1$, we have $b(G) = b$;*
(ii) *If b is a positive integer satisfying $2 \leq k \leq b-1$, then for all values of n satisfying*

$$\left\lfloor \frac{(b-1)(k+1)}{2} \right\rfloor < n+1 < \left\lfloor \frac{b(k+1)}{2} \right\rfloor,$$

we have $b(G) = b$.

Thus we have precise values for the base size of S_n acting on k-subsets, provided that $n \geq \frac{k(k+1)}{2} + 1$.

In her (also unpublished) 2005 Ph.D. thesis [**13**], Benbenishty also obtained bounds on the base size of the symmetric group acting on k-subsets. (We would like to thank the referee for directing us to her results.)

PROPOSITION 2.26 (Benbenishty [**13**]). *Let G denote the action of S_n on k-subsets of $\{1, \ldots, n\}$, and let $n = rk + d$. Then:*

(i) *When $n \geq k^2$, we have $b(G) \leq r + k\lfloor r/k \rfloor + d$;*
(ii) *When $n < k^2$, and where $c = \lfloor \log_r k \rfloor$, we have $b(G) \leq 3r(c+1)$.*

The bounds in Proposition 2.26(i) (for $n \geq k^2$) are not quite as strong as in Theorems 2.22 and 2.25, although for larger values of k they are asymptotically similar: the bound is approximately $2\lfloor n/k \rfloor$, compared that of $2\lfloor (n-1)/(k+1) \rfloor$. However, the focus here was to verify Pyber's conjecture (see subsection 2.1 above) for these groups, rather than obtain exact values. Also, Proposition 2.26(ii) gives bounds for when $n < \frac{k(k+1)}{2} + 1$, where Theorems 2.22 and 2.25 do not apply.

In [**58**], Gibbons and Laison consider some problems about bases of automorphism groups of graphs (although they used the terms fixing set and fixing number). They give a greedy algorithm for finding bases (build a base by successively choosing vertices from the largest orbit of the stabiliser of the points previously chosen). This algorithm is exactly the same as that given, for permutation groups in general, by Blaha [**15**] in 1992. This algorithm always produces a base which is irredundant.

Gibbons and Laison ask if there exists a graph for which the greedy algorithm always gives a base strictly larger than the minimum possible. In [**33**], Section 4.13, it is shown that for the symmetric group S_n in its action on the 2-subsets of $\{1, \ldots, n\}$ the greedy algorithm returns a base of size $\sim \frac{3}{4}n$. This contrasts with Proposition 2.24, which shows the minimum base size to be $\sim \frac{2}{3}n$. Of course, this action is precisely the automorphism group of $J(n, 2)$ and $K(n, 2)$, so these graphs provide infinite families of examples which answer Gibbons and Laison's question.

While this example shows that the greedy algorithm does not always succeed, it does provide a reasonable approximation. In [**15**], Blaha showed that if G has degree n, then the greedy algorithm produces an irredundant base of size $O(b(G) \log \log n)$.

2.6. *The exchange property and IBIS groups*

Given that bases for groups are a generalisation of bases for vector spaces, it is natural to ask which properties of vector space bases are carried over. One such property is the "exchange property". Namely, given two bases B_1 and B_2 for a vector space V and an element $x \in B_1 \setminus B_2$, does there exist $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\}$ is also a base? A pair $(\Omega, \mathcal{B})$, where $\mathcal{B}$ is a non-empty family of subsets of a set Ω satisfying this axiom, is called a *matroid*. (This is only one of a number of equivalent definitions of a matroid: see Oxley [**81**] for details.) The members of $\mathcal{B}$ are called the *bases* of the matroid. The bases of a vector space provide a natural motivating example.

The exchange property was first investigated for bases of permutation groups by Cameron and Fon-Der-Flaass in their 1995 paper [**35**]. They proved the following theorem:

THEOREM 2.27 (Cameron and Fon-Der-Flaass [**35**]). *Suppose G is a permutation group acting on a set Ω. Then the following are equivalent:*

(i) *the irredundant bases of G have the same size;*
(ii) *the irredundant bases of G are preserved by re-ordering;*
(iii) *the irredundant bases of G form the bases of a matroid.*

A group satisfying the conditions in Theorem 2.27 is called an *IBIS group*; the acronym stands for "Irredundant Bases of Invariant Size". As observed earlier, any minimal base is irredundant, so it follows that the minimal bases of an IBIS group must also be equicardinal. (In fact, it is straightforward to verify that condition (ii) is equivalent to every irredundant base being minimal.) Examples of IBIS groups include the base-transitive groups we mentioned in subsection 2.3.

More recently, Boutin [**21**] has investigated graphs for which the minimum determining sets (i.e. bases) have the exchange property. In other words, this is studying which graphs have automorphism groups which are IBIS groups. In particular, she considers outerplanar graphs, and obtains a criterion for when the automorphism group of an outerplanar graph is an IBIS group. She also shows that the automorphism groups of trees and of wheels are IBIS groups.

One of the results obtained by Cameron and Fon-Der-Flaass [**35**] is a characterisation of the IBIS groups for which the matroid obtained is the uniform matroid $U_{k,n}$ (i.e. the matroid on $\{1, \ldots, n\}$ for which every k-subset is a base: see Oxley [**81**], Example 1.2.7). They showed that such a group is necessarily $(k-1)$-transitive. Since the only graphs with 2-transitive automorphism groups are complete, then (other than the symmetric group S_n acting on K_n) the only possibility for automorphism groups of graphs are when the uniform matroid has rank 2. In this case (i.e. any pair of points is a base for the group G), the groups are precisely the Frobenius groups (see Dixon and Mortimer [**44**], Section 3.4).

Burnside's theorem on groups of prime degree states that a transitive group of prime degree which is not 2-transitive is a Frobenius group (see Dixon and Mortimer [**44**], Section 3.5). Thus we have the following result.

PROPOSITION 2.28. *Let p be a prime, and let Γ be a vertex-transitive graph with p vertices (other than a complete graph or null graph). Then* $\mathrm{Aut}(\Gamma)$ *is an IBIS group, for which the associated matroid is the uniform matroid $U_{2,p}$ (i.e. any pair of vertices is a base for* $\mathrm{Aut}(\Gamma)$*).*

Proof. Since Γ is not complete, $\mathrm{Aut}(\Gamma)$ is not 2-transitive, so by Burnside's theorem $\mathrm{Aut}(\Gamma)$ is a Frobenius group. Thus any pair of vertices forms a base, and therefore $\mathrm{Aut}(\Gamma)$ is an IBIS group associated with the uniform matroid $U_{2,p}$. □

EXAMPLE 2.29. Suppose q is a prime power such that $q \equiv 1 \pmod 4$. Then the *Paley graph* P_q has vertex set $\mathbb{F}_q$, and x is adjacent to y if and only if $x - y$ is a quadratic residue (i.e. non-zero square) in $\mathbb{F}_q$.

It is easy to see that the Paley graph is vertex-transitive. Thus when the number of vertices is a prime p, Proposition 2.28 shows that $\mathrm{Aut}(P_p)$ is an IBIS group associated with the uniform matroid $U_{2,p}$.

Paley graphs will reappear as examples later in this paper.

3. *Metric and other dimensions*

3.1. *Metric dimension*

The metric dimension is a well-known parameter in graph theory. It was first introduced in the 1970s, independently by Harary and Melter [**62**] and by Slater [**90**].

DEFINITION 3.1. A *resolving set* for a graph $\Gamma = (V, E)$ is a set of vertices $S = \{v_1, \ldots, v_k\}$ such that for all $w \in V$, the ordered list of distances $\mathcal{D}(w|S) = (d(w, v_1), \ldots, d(w, v_k))$ (corresponding to an arbitrary ordering of S) uniquely determines w.

That is, S is a resolving set for Γ if for any pair of vertices u, w, $\mathcal{D}(u|S) = \mathcal{D}(w|S)$ if and only if $u = w$.

DEFINITION 3.2. The *metric dimension* of Γ, denoted $\mu(\Gamma)$, is the smallest size of a resolving set for Γ.

EXAMPLE 3.3. Recall the Petersen graph from Example 2.21. It is straightforward to check that $\{12, 13, 14\}$ is a resolving set for the Petersen graph, and that its metric dimension is 3.

The notion of metric dimension makes sense in any metric space. For instance, in Euclidean space, the metric dimension is precisely the affine dimension, so it really is a "dimension" in a geometric sense. In graph theory, it is a parameter that has appeared in various applications, as diverse as combinatorial optimisation [**85**], pharmaceutical chemistry [**39**], robot navigation [**71**] and sonar [**90**], to name but a few. The paper by Hernando *et al.* [**63**] contains a considerable bibliography.

Computing the metric dimension of a graph is an NP-hard problem: it is one of the examples given in the book by Garey and Johnson [**57**] (Appendix A1, GT61), while a proof of this is given by Khuller *et al.* in [**71**]. Indeed, the problem is one of the computationally hard problems that have had genetic algorithms applied to them: see Kratica *et al.* [**73**] for details.

As with base size, metric dimension is a subject rife with non-standard terminology. For example, resolving sets are also known as *locating sets* [**90**], *metric generators* [**85**], *metric bases* [**62**], or even just *bases* [**70**], minimum resolving sets known as *reference sets* [**90**] and the metric dimension also known as the *locating number* [**90**] or the *rigidity* [**70**] of a graph. In addition, as we shall see later, various other parameters turn out to be equivalent to metric dimension in certain cases.

The following results are straightforward, and proofs can be found in Chartrand *et al.* [**39**], for instance.

PROPOSITION 3.4. *Suppose a graph Γ has n vertices and diameter d. Then $\mu(\Gamma) \leq n - d$.*

PROPOSITION 3.5. *A graph on n vertices has metric dimension $n-1$ if and only if it is complete.*

An implicit lower bound on $\mu(\Gamma)$ can be obtained by considering the maximum possible number of vertices of a graph with diameter d and metric dimension k. The following result is also straightforward.

PROPOSITION 3.6. *The suppose Γ is a graph with n vertices, diameter d and metric dimension k. Then $n \leq k + d^k$.*

Proof. Let S be a resolving set. If $y \in S$, then there are exactly k possibilities for $\mathcal{D}(y|S)$; if $y \notin S$, then there are d^k possibilities for $\mathcal{D}(y|S)$. □

A generalisation of this bound has been given by Hernando *et al.* [**63**].

THEOREM 3.7 (Hernando *et al.* [**63**]). *Suppose Γ is a graph with n vertices, diameter d and metric dimension k. Then*

$$n \leq \left(\left\lfloor \frac{2d}{3} \right\rfloor + 1 \right)^k + k \sum_{i=1}^{\lceil d/3 \rceil} (2i-1)^{k-1}.$$

This is indeed a generalisation: the two bounds agree when $d = 2$ and $d = 3$, and thereafter it is stronger. Hernando *et al.* also go on to show that this bound is sharp, by constructing a graph which meets this bound for each $d \geq 2$ and $k \geq 1$.

In [**43**], Cvetković *et al.* called a graph which meets the upper bound in Proposition 3.6 *distance-perfect*. They showed that such graphs are rare: a distance-perfect graph is either complete, or has diameter at least 3; Theorem 3.7 implies that there are no distance-perfect graphs of diameter $d \geq 4$.

3.2. *Base size and metric dimension*

Bringing the two main strands of this paper together, we see that metric dimension and base size are related, thanks to the following straightforward result.

PROPOSITION 3.8. *A resolving set for Γ is a base for* $\mathrm{Aut}(\Gamma)$.

Proof. Let $S = (x_1, \ldots, x_k)$ be an (ordered) resolving set for Γ, and let $G = \mathrm{Aut}(\Gamma)$. We will show that the pointwise stabiliser of S in G is trivial.

Choose a vertex $v \in V(\Gamma)$; since S is a resolving set, the vector of distances $(d(v, x_1), \ldots, d(v, x_k))$ is unique. However, for any $g \in G$, $d(v, x_i) = d(v^g, x_i^g)$, and thus if g fixes each $x_i \in S$, it must also fix v. Hence $g \in \bigcap_{v \in V(\Gamma)} G_v$, and since the action is faithful, this is trivial. □

As a consequence, the following corollary is obvious.

COROLLARY 3.9. *For any graph* Γ, $b(\mathrm{Aut}(\Gamma)) \leq \mu(\Gamma)$.

Thus it is possible to use the metric dimension of a graph to bound the base size of its automorphism group. However, the bound is not always a good one: as we will see in Section 4, there are examples of families of graphs where the difference between the two parameters can be made arbitrarily large.

Given the relationship between the metric dimension of a graph and the base size of its automorphism group, one could ask if there is an analogue of metric dimension for arbitrary permutation groups. In order for us to address this, we need first to discuss coherent configurations, which we do now.

3.3. *Coherent configurations and association schemes*

The *orbitals* of a permutation group G are its orbits on $\Omega \times \Omega$. There are two types of orbital: *diagonal* (orbits on pairs of the form (x, x)) and *non-diagonal* (orbits on pairs of the form (x, y) where $x \neq y$). If the group is transitive, then there is only one diagonal orbital, and the non-diagonal orbitals are in a one-to-one correspondence with the *suborbits* of G, i.e. the orbits of the stabiliser of a point. The number of orbitals is the *rank* of G. (See Dixon and Mortimer [**44**], Section 3.2, for further details.)

We can think of the orbitals of G as a partition of $\Omega \times \Omega$ into a set of binary relations on Ω; label these relations as $\mathcal{R} = \{R_1, \ldots, R_t\}$ (where t is the rank of G). Now, the relations satisfy the following three conditions:

CC1. There is a subset of $\mathcal{R}$ which partitions $\{(x, x) \mid x \in \Omega\}$.
CC2. For each $R_i \in \mathcal{R}$, its transpose $R_i^* = \{(y, x) \mid (x, y) \in R_i\} \in \mathcal{R}$.
CC3. For any $i, j, k \in \{1, \ldots, t\}$, given a pair $(x, y) \in R_k$, the number of points $z \in \Omega$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is dependent only on i, j and k, not on the choice of (x, y). (We denote this number by p_{ij}^k.)

DEFINITION 3.10. Suppose Ω is a finite set, and that $\mathcal{R}$ is a partition of $\Omega \times \Omega$. Then $(\Omega, \mathcal{R})$ is a *coherent configuration* if and only if conditions CC1–CC3 are satisfied.

Often we will just denote a coherent configuration by $\mathcal{R}$. They were defined by D. G. Higman [**64**] as a means of studying finite permutation groups. (For a detailed treatment of coherent configurations, and their relationship to permutation groups, see Chapter 3 of [**33**]; for an interesting account of their development, see the biography of Higman by Bannai *et al.* [**11**].) However, not all coherent configurations arise as the orbitals of a permutation group: if one does, then it is called *Schurian*, and we denote it by $\mathcal{R}(G)$.

The *rank* of a coherent configuration is the number of relations, while the numbers p_{ij}^k are called the *intersection numbers* of $\mathcal{R}$. We say that a coherent configuration is *homogeneous* if the whole of the diagonal subset $\{(x, x) \mid x \in \Omega\}$ is a single relation R_1 (a strengthening of CC1). Furthermore, a coherent configuration is an *association scheme* if it satisfies $R_i^* = R_i$ for all i (a strengthening of CC2). Note that:

- an association scheme is necessarily a homogeneous coherent configuration (see [**64**]);
- the coherent configuration arising from a permutation group G is homogeneous if and only if G is transitive, and is an association scheme if and only if G is *generously transitive* (that is, any two points of Ω can be interchanged by an element of G.

The reader should be aware that the term "association scheme" is not used consistently in the literature. We use the same definition as the books of Bailey [**7**] and Brouwer, Cohen and Neumaier [**22**]; however, the books by Bannai and Ito [**12**] and Zieschang [**96**] each give different

definitions, which are both weaker than ours. We refer the reader to [**34**] for a discussion of the various objects that have been called "association schemes".

There are several equivalent ways of understanding coherent configurations (and association schemes). We can visualise them by regarding the relations $\{R_1, \ldots, R_t\}$ as "colours", and thus the coherent configuration as a "colouring" of $\Omega \times \Omega$.

EXAMPLE 3.11. Figure 4 depicts a coherent configuration of rank 3 on 4 points.

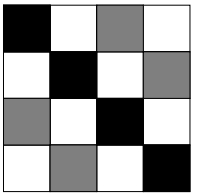


FIGURE 4. *A coherent configuration of rank 3.*

Another approach is to think of $\mathcal{R}$ as a colouring of the arcs of a complete directed graph with vertex set Ω. Thus each of the relations R_i becomes the arc set of a directed graph. (Note that if $\mathcal{R}$ is an association scheme, then the graphs are undirected.) A coherent configuration is said to be *primitive* if each of the digraphs corresponding to non-diagonal relations are connected. A well-known result of Higman [**64**] shows that G is a primitive group if and only if $\mathcal{R}(G)$ is a primitive coherent configuration.

An alternative way of studying coherent configurations is to view them purely algebraically. Suppose $\mathcal{R} = \{R_1, \ldots, R_t\}$ is a coherent configuration. For each relation R_i, we define an $\Omega \times \Omega$ matrix A_i, where the (x, y)-entry is 1 if and only if $(x, y) \in R_i$, and all other entries are 0. Now, these matrices satisfy the following conditions:

CC1′. A subset of $\mathcal{A} = \{A_1, \ldots, A_t\}$ sums to the identity matrix.
CC2′. For each A_i, its transpose $A_i^T \in \mathcal{A}$.
CC3′. Any product $A_i A_j$ is an integer linear combination of the matrices in $\mathcal{A}$.

These conditions are equivalent to the three in the definition of a coherent configuration. We also notice that the sum of the A_i is the all-ones matrix J.

The complex algebra generated by $\mathcal{A}$ is called a *cellular algebra*. Cellular algebras were introduced by Weisfeiler and Leman in the late 1960s [**95**], independently of Higman, and have been studied extensively in this form in the former Soviet Union (see the book by Faradžev *et al.* [**54**]). In the case where $\mathcal{R}$ is an association scheme, the algebra is usually called the *Bose–Mesner algebra* of the scheme. (We remark that these cellular algebras are not the same as those introduced much later by Graham and Lehrer [**61**].)

3.4. *Class dimension and orbital dimension*

The next definition gives us an analogue of metric dimension for coherent configurations. Let $C(x, y)$ denote the relation containing the pair (x, y) (i.e. the "colour" of that pair).

DEFINITION 3.12. A *resolving set* for a coherent configuration $\mathcal{R}$ is a set of points $S = \{x_1, \ldots, x_k\} \subseteq \Omega$ such that for all $y \in \Omega$, the ordered list of colours $\mathcal{O}(y|S) = (C(y, x_1), \ldots, C(y, x_k))$ is unique.

That is, S is a resolving set for $\mathcal{R}$ if for any pair of points y, z, $\mathcal{O}(y|S) = \mathcal{O}(z|S)$ if and only if $y = z$.

DEFINITION 3.13. The *class dimension* of a coherent configuration $\mathcal{R}$, denoted $\mu(\mathcal{R})$ is the smallest size of a resolving set for $\mathcal{R}$. Where the coherent configuration consists of the orbitals of a permutation group G, we call this invariant the *orbital dimension* of G and denote it by $\mu(G)$.

Resolving sets for coherent configurations were first introduced by Babai in 1981 [**5**] by the name *distinguishing sets*, and the class dimension was called the *distinguishing number*. As we saw in in subsection 2.2, this term has recently become widespread in graph theory for a different object, so we have avoided this term. Also, in their account of Babai's paper, Dixon and Mortimer ([**44**], Section 5.3) used the term *discriminating set* instead.

The following is a direct analogue of Proposition 3.8.

PROPOSITION 3.14. *A resolving set for a permutation group G is a base for G.*

This is proved in exactly the same manner as Proposition 3.8, replacing "distance from x to y" with "orbital containing x and y". It was an important device in Babai's paper [**5**], where he was able to bound the class dimension of primitive coherent configurations of rank at least 3, used this to bound the base size of primitive permutation groups, and then used this to bound the order of such groups. We give Babai's most general bound below.

THEOREM 3.15 (Babai [**5**]). *Let $\mathcal{R}$ be a primitive coherent configuration of rank at least 3 on n points. Then the class dimension $\mu(\mathcal{R})$ satisfies $\mu(\mathcal{R}) < 4\sqrt{n}\log n$.*

The reason for avoiding the rank 2 case in 3.15 is that this case can easily be dealt with. The next two results are analogues of Propositions 3.4 and 3.5 for metric dimension. Note that while they only apply to homogeneous coherent configurations, a coherent configuration of rank 2 is automatically homogeneous.

PROPOSITION 3.16. *Let $\mathcal{R}$ be a homogeneous coherent configuration of rank t on n points. Then $\mu(\mathcal{R}) \leq n - t + 1$.*

Proof. Choose a point $u \in \Omega$, and a set of points $W = \{v_1, \ldots, v_{t-1}\}$ distinct from u so that the colours $C(u, v_i)$ are all distinct. (The fact that $\mathcal{R}$ is homogeneous ensures that this is possible.) Then the set $W = \Omega \setminus \{v_1, \ldots, v_{t-1}\}$ is a resolving set for $\mathcal{R}$: if $x \in W$, then there is a unique appearance of $C(x, x)$ in $\mathcal{O}(x|W)$, while for each $x \notin W$, the entry in $\mathcal{O}(x|W)$ corresponding to u will be distinct. □

REMARK. As Babai has pointed out to the authors, the bound in Proposition 3.16 is tight for every value of t and when n is divisible by $t - 1$. The coherent configuration arising from the group $S_k \wr C_{t-1}$ (in the imprimitive action) provides an example, with $n = (t-1)k$.

Babai also points out that the methods of [**5**] can be used to show that, with possibly a finite number of exceptions, if $\mathcal{R}$ is a homogeneous coherent configuration of rank at least 3 on n vertices where n is composite, then $\mu(\mathcal{R}) \leq n - p(n)$, where $p(n)$ is the smallest prime divisor of n. He conjectures that there are no exceptions.

PROPOSITION 3.17. *Let $\mathcal{R}$ be a homogeneous coherent configuration on n points. Then $\mu(\mathcal{R}) = n - 1$ if and only if $\mathcal{R}$ has rank 2.*

Proof. First, suppose $\mathcal{R}$ has rank 2. Label the two relations as 0 (for the diagonal entries) and 1 (for the non-diagonal entries). Suppose S is a resolving set for $\mathcal{R}$. For any $x \notin S$, all entries of $\mathcal{O}(x|S)$ will be 1, so we can have at most one point outside of a resolving set, and so $\mu(\mathcal{R}) \geq n - 1$. Applying the upper bound from Proposition 3.16 above, it follows that $\mu(\mathcal{R}) = n - 1$.

Conversely, suppose $\mathcal{R}$ has rank $t \geq 3$. Then by Proposition 3.16, $\mu(\mathcal{R}) \leq n - t + 1 \leq n - 2$. □

Since a permutation group has rank 2 if and only if it is 2-transitive, we have the following corollary for orbital dimension.

COROLLARY 3.18. *Let G be a group of degree n. Then $\mu(G) = n - 1$ if and only if G is 2-transitive.*

Continuing the analogy, as with metric dimension we can also obtain an implicit lower bound for the class dimension, similar to Proposition 3.6.

PROPOSITION 3.19. *Let $\mathcal{R}$ be a coherent configuration on n points of rank t, with s diagonal classes, and let $\mu(\mathcal{R}) = k$. Then $n \leq k + (t - s)^k$.*

Proof. Let S be a resolving set. If $y \in S$, then $\mathcal{O}(y|S)$ contains an entry from a diagonal class and there are exactly k possibilities for it; otherwise, if $y \notin S$, then $\mathcal{O}(y|S)$ contains only non-diagonal classes, and so there are $(t - s)^k$ possibilities for it. □

3.5. *Distance-transitive and distance-regular graphs*

The class of distance-transitive graphs is particularly interesting in this context, as it is precisely where our three "dimensions" all coincide. They are defined as follows.

DEFINITION 3.20. A graph Γ is *distance-transitive* if for all vertices u, v, u', v' such that $d(u, v) = d(u', v')$, there exists $g \in \mathrm{Aut}(\Gamma)$ such that $u^g = u'$ and $v^g = v'$.

In other words, $\mathrm{Aut}(\Gamma)$ acts transitively on pairs of vertices at a given distance. We refer the reader to Biggs' book [**14**] for background material on distance-transitive graphs.

Now, it follows from the definition that the orbitals of $\mathrm{Aut}(\Gamma)$ are precisely the pairs of vertices at each distance, so the rank of $\mathrm{Aut}(\Gamma)$ is $d + 1$, where d is the diameter of Γ. Thus we can label the orbitals as $\{R_0, R_1, \ldots R_d\}$, where $(u, v) \in R_i$ if and only if $d(u, v) = i$. Thus $R_i^* = R_i$ for all i, so the coherent configuration arising from $\mathrm{Aut}(\Gamma)$ is symmetric, and therefore is an association scheme. Consequently, we have the following.

PROPOSITION 3.21. *Let Γ be a graph such that $G \leq \mathrm{Aut}(\Gamma)$ acts distance-transitively on the vertex set V. Then the orbital dimension of G is equal to the metric dimension of Γ.*

If we weaken the hypotheses so to ask merely for graphs for which the sets of pairs of vertices at each distance form an association scheme, we obtain the class of *distance-regular graphs* (see Brouwer, Cohen and Neumaier [**22**] for full details). In this case, the metric dimension of such a graph is the class dimension of the association scheme, and thus Babai's bound (Theorem 3.15) gives a bound on the metric dimension of a distance-regular graph on n vertices. However, Babai's paper contains a number of other results which can be applied here.

Suppose Γ is a distance-regular graph with n vertices, valency k and diameter d. Following Biggs' notation [**14**], for a given vertex $v \in V$, we let $\Gamma_i(v) = \{w \in V \mid d(v,w) = i\}$, and define $k_i = |\Gamma_i(v)|$. Where $w \in \Gamma_i(v)$, let c_i denote the number of neighbours of w at distance $i-1$ from v, a_i the number of neighbours of w at distance i from v, and b_i the number of neighbours of w at distance $i+1$ from v. That Γ is distance-regular assures that these numbers are constants. We put these numbers in an array, called the *intersection array* of Γ,

$$\iota(\Gamma) = \left\{ \begin{array}{ccccc} * & c_1 & \cdots & c_{d-1} & c_d \\ a_0 & a_1 & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & \cdots & b_{d-1} & * \end{array} \right\}.$$

The $*$ indicate that c_0 and b_d are undefined. It is easy to see that $a_0 = 0$, $b_0 = k$, $c_1 = 1$, and to deduce that $k_i b_i = k_{i+1} c_{i+1}$. Hence the numbers $k_1, \ldots, k_d$ can be obtained from $\iota(\Gamma)$.

The following result is due to Babai, and holds for primitive coherent configurations in full generality; we state his result as it holds for distance-regular graphs.

THEOREM 3.22 (Babai [**5**]). *Let Γ be a primitive distance-regular graph on n vertices of diameter d. Then the metric dimension of Γ satisfies*

$$\mu(\Gamma) < 2d \frac{n}{n-M} \log n$$

(where $M = \max\{k_1, \ldots k_d\}$).

Thus this result gives an upper bound on the metric dimension of a primitive distance-regular graph, which can be obtained from its intersection array. We remark that the imprimitive distance-regular graphs have a straightforward characterisation (known as *Smith's Theorem*, after D. H. Smith [**91**] who proved it for distance-transitive graphs): a distance-regular graph of valency at least 3 is imprimitive if and only if it is either bipartite or antipodal. (A graph Γ of diameter d is *antipodal* if for any $u, w \in \Gamma_d(v)$, we have $d(u,w) = d$.) For a proof, see Theorem 4.2.1 of Brouwer, Cohen and Neumaier [**22**].

Many of the families of graphs for which metric dimension (or equivalent parameters) have been investigated are distance-transitive. We discuss some of these families below.

3.6. *Hamming graphs, coin-weighing and Mastermind*

Consider the Hamming graphs $H(d,q)$ which we saw in subsection 2.4. These are a classical example of distance-regular graphs, and the association scheme arising is called the *Hamming scheme*. Recall that the hypercube $H(d,2)$ is a special case of a Hamming graph. In [**39**], Chartrand *et al.* obtained an upper bound on the metric dimension of the hypercube. This was improved by Sebő and Tannier, who realised that it is equivalent to solving a coin-weighing problem posed by Erdős and Rényi [**47**] in 1963 and solved by Lindström [**79**] in 1964.

THEOREM 3.23 (Lindström [**79**]; Sebő and Tannier [**85**]). *The metric dimension of the hypercube $H(d,2)$ satisfies*

$$\mu(H(d,2)) = \frac{2d}{\log_2 d}(1 + o(1)).$$

Since $H(d,2)$ is distance-transitive, the metric dimension of the hypercube is equal to the orbital dimension of its automorphism group $S_2 \wr S_d$ (acting in the product action). Of course, this is also the class dimension of the Hamming scheme $H(d,2)$.

For the general Hamming scheme $H(d,q)$, bounds follow from the work of Chvátal [**40**] on strategies for the game *Mastermind*. In this game, the first player chooses a "mystery" vector $\mathbf{m} = [m_1, \ldots, m_d]$ over an alphabet of size q. (In the game, where d is usually 4 or 5 and $q = 6$, the vector is represented by d pins in q colours.) The second player then successively chooses "response" vectors $\mathbf{r} = [r_1, \ldots, r_d]$, in an attempt to deduce the mystery vector; at each stage, his opponent provides two pieces of information, namely (i) the number a of positions where $\mathbf{m}$ and $\mathbf{r}$ agree, and (ii) the total number b of pins of the correct colour but in the wrong position.

Now, the mystery vector $\mathbf{m}$ and the response vectors $\mathbf{r}$ are vertices of the Hamming scheme $H(d,q)$, and the number $d - a$ is the Hamming distance between $\mathbf{m}$ and $\mathbf{r}$. Thus, if the response vectors chosen are a resolving set for $H(d,q)$ of size k, then (in theory at least) after k responses the player will be able to deduce $\mathbf{m}$. Thus the metric dimension of $H(d,q)$ provides an upper bound on the number of guesses $f(d,q)$ needed for a successful deduction.

Chvátal obtained an upper bound on $f(d,q)$, which is valid when q is small when compared to d. As his proof only uses the first piece of information, a, this also gives an upper bound on $\mu(H(d,q))$. This is another asymptotic result.

THEOREM 3.24 (Chvátal [**40**]). *Given $\varepsilon > 0$, there exists an integer d_ε such that if $d > d_\varepsilon$ and $q < d^{1-\varepsilon}$, then the metric dimension of $H(d,q)$ satisfies*

$$\mu(H(d,q)) \leq (2+\varepsilon) d \frac{1 + 2\log_2 q}{\log_2 d - \log_2 q}.$$

Kabatianski *et al.* [**70**] have reported improved bounds for the metric dimension of $H(d,3)$ and $H(d,4)$; however, this was published only in an extended abstract, with all proofs omitted. Cáceres *et al.* [**30**] have also studied the problem, for $H(2,m)$ (the square lattice graphs). They obtained the following exact result, as part of an investigation into the metric dimension of Cartesian products of graphs.

THEOREM 3.25 (Cáceres *et al.* [**30**]). *For all $m \geq 1$, the metric dimension of the square lattice graph $H(2,m)$ is $\mu(H(2,m)) = \lfloor \frac{2}{3}(2m-1) \rfloor$.*

3.7. *Separation index and strongly regular graphs*

In [**93**], Vince defines the *separation index* of a finite permutation group G acting on a set Ω, which is defined in terms of partitions. The set of all partitions of Ω forms a lattice, ordered by refinement, and the unique minimal element is the partition $\mathbf{0}$ into singletons. For $x \in \Omega$, let $\pi(x)$ denote the partition of Ω into the orbits of the point stabiliser G_x (i.e. suborbits).

DEFINITION 3.26. A subset $S = \{x_1, \ldots, x_k\}$ of Ω is said to *separate* G if in the lattice of all partitions of Ω, the meet

$$\bigwedge_{x \in S} \pi(x) = \mathbf{0}.$$

The *separation index* of G, denoted $\sigma(G)$, is the smallest cardinality of a separating set.

Vince goes on to define the separation index of a graph to be that of its automorphism group, and then the separation index of a surface to be the largest separation index of a 3-connected graph embedded in that surface. Vince's main result is that the separation index of the sphere is 3. (Further results in this topological setting have been obtained by Fijavž and Mohar [**56**].)

Now, in the case where G is transitive, because of the correspondence between suborbits and orbitals, the separation index is precisely the orbital dimension, as the next proposition shows.

PROPOSITION 3.27. *Let G be a transitive permutation group on Ω. Then a subset $S \subseteq \Omega$ is a separating set for G if and only if it is a resolving set for G, and so $\sigma(G) = \mu(G)$.*

Proof. Let $S = \{x_1, \ldots, x_k\}$, and suppose it is a separating set for G. Thus for all $y, z \in \Omega$, if y and z belong to $\pi(x_i)$ for all i, then $y = z$ (as otherwise, $\bigwedge_{x \in S} \pi(x)$ would contain a part of size greater than 1). So if for all i the orbital containing (y, x_i) is the same as that containing (z, x_i) (i.e. if $\mathcal{O}(y|S) = \mathcal{O}(z|S)$) then $y = z$. Hence S is a resolving set for G.

The reverse implications work identically. □

In particular, if G is the automorphism group of a distance-transitive graph Γ, then the separation index of G is equal to the metric dimension of Γ. We note also that a separating set is a base for G (even if G is intransitive).

In [**55**], Fijavž and Mohar considered the separation index of the Paley graph P_p (recall Example 2.29). They obtained upper and lower bounds on $\sigma(P_p)$ where p is prime. Since Paley graphs are distance-transitive, then these bounds hold for their metric dimension.

THEOREM 3.28 (Fijavž and Mohar [**55**]). *Let p be a prime satisfying $p \equiv 1 \pmod 4$. Then the metric dimension of the Paley graph P_p satisfies*

$$\lfloor \log_2 p \rfloor \leq \mu(P_p) \leq \lfloor 2 \log_2 p \rfloor.$$

The lower bound, which is true for all graphs of diameter 2, is immediate from Proposition 3.4. The upper bound turns out to follow from a much more general result due to Babai [**4**] about arbitrary graphs. For a graph Γ, let $m(\Gamma)$ denote the largest integer with the property that the symmetric difference $|N(u) \triangle N(v)| \geq m$ for all distinct vertices u, v of Γ.

PROPOSITION 3.29 (Babai [**4**]). *Let Γ be a graph with n vertices. Then*

$$\mu(\Gamma) \leq \frac{2 \log n}{1 - \log(1 - m(\Gamma)/n)},$$

which implies that $\mu(\Gamma) \leq 2n \log n / m(\Gamma)$.

This is particularly useful in the case of strongly regular graphs, which we define now.

DEFINITION 3.30. A connected, regular graph Γ with n vertices and valency k is said to be *strongly regular* if:

– each pair of adjacent vertices has a constant number a of common neighbours;
– each pair of non-adjacent vertices has a constant number c of common neighbours.

The integers (n, k, a, c) are called the *parameters of* Γ.

It follows from the definition that a connected graph is strongly regular if and only if it is distance-regular and its diameter is 2; as association schemes these have rank 3, and in fact every rank 3 association scheme arises in this way. A rank 3 permutation group is therefore contained in the automorphism group of some distance-transitive graph of diameter 2; such graphs are known as *rank 3 graphs*, and Paley graphs form examples of these. From the parameters (n, k, a, c), all the intersection numbers of the corresponding association scheme can be obtained. (See Chapter 2 of [**37**] for further background material.)

A strongly regular graph is *primitive* if and only if the corresponding association scheme is primitive. However, the only imprimitive strongly regular graphs are the complete multipartite graphs.

In a primitive strongly regular graph with parameters (n, k, a, c), it is straightforward to see that $m(\Gamma) = \min\{2(k-a-1), 2(k-c)\}$. Using this, Babai [**5**] showed the following. (This a special case of the bound for primitive distance-regular graphs we saw in Theorem 3.22 above.)

THEOREM 3.31 (Babai [**5**]). *Let Γ be a primitive strongly regular graph with n vertices and valency $k < \frac{1}{2}n$. Then*

$$\mu(\Gamma) < \frac{2n^2 \log n}{k(n-k)} < \frac{4n \log n}{k}.$$

In the special case of the Paley graph P_p, we have $m(\Gamma) = (p-1)/2$, and the upper bound of Theorem 3.28 follows.

There are also some computational results on the metric dimension of strongly regular graphs, due to Kratica *et al.* [**72**]. Using an integer programming formulation of the metric dimension problem due to Currie and Oellermann [**42**], and the online catalogue of strongly regular graphs due to Spence [**92**], they were able to calculate the metric dimension of every strongly regular graph on up to 45 vertices. In a vast majority of cases, the metric dimension is determined by the parameters of the graph (for instance, all 32,548 strongly regular graphs with parameters $(36, 15, 6, 6)$ have metric dimension 6), or when different values are possible, they differ by 1 (for instance, of the 41 strongly regular graphs with parameters $(29, 14, 6, 7)$, 40 have metric dimension 5 and one has metric dimension 6). It would be interesting to find a theoretical explanation of these phenomena.

3.8. *Johnson and Kneser graphs*

Recall the Johnson graphs from subsection 2.5. The Johnson graph $J(n, k)$ is another classical example of a distance-transitive graph. When $n > 2k$, the Johnson graph is primitive; when $n = 2k$, it is antipodal (since each vertex has a unique antipode) and thus imprimitive. In this case, the automorphism group $\mathrm{Aut}(J(2k, k))$ is $S_n \times C_2$ (the extra automorphisms being those interchanging a k-subset with its complement). The corresponding association scheme, the *Johnson scheme*, is precisely the coherent configuration arising from the action of the symmetric group S_n on k-subsets. By abuse of notation, we will also denote the Johnson scheme by $J(n, k)$.

The Kneser graph is not distance-transitive in general. One case where it is distance-transitive is when $k = 2$ (for $n \geq 5$): the graph $K(n, 2)$ is the complement of the Johnson graph $J(n, 2)$, and both are distance-transitive graphs of diameter 2. Another example of a distance-transitive Kneser graph is $K(2k-1, k-1)$, known as the *odd graph* O_k (see Biggs [**14**]); the odd graph O_3 is the Petersen graph.

In the remainder of this subsection, we will consider the case $k = 2$ only. Recall Proposition 2.24, which gives the base size of the symmetric group in its action on 2-subsets to be around $\frac{2}{3}n$. By Proposition 3.14, this gives a lower bound on the class dimension of the Johnson

scheme $J(n,2)$, and thus the metric dimension of both the Johnson graph $J(n,2)$ and Kneser graph $K(n,2)$. We shall see that, unlike the Hamming graphs, this bound can actually be met infinitely often.

THEOREM 3.32. *Let G denote the action of S_n on 2-subsets of $\{1,\ldots,n\}$, where $n \geq 6$. Then for the orbital dimension $\mu(G)$, we have:*

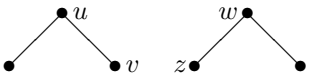
(i) *For $n \equiv 0 \pmod 3$, $\mu(G) = b(G) = \frac{2}{3}n$;*
(ii) *For $n \equiv 1 \pmod 3$, $\mu(G) = b(G) + 1 = \frac{2}{3}(n-1) + 1$;*
(iii) *For $n \equiv 2 \pmod 3$, $\mu(G) = b(G) + 1 = \frac{2}{3}(n-2) + 2$.*

Proof. As in Proposition 2.24, we think of the 2-subsets of $\{1,\ldots,n\}$ as the edges of a complete graph K_n. First, we consider case (i), where $n \equiv 0 \pmod 3$. Let S be (the edges of) a spanning subgraph of K_n as depicted in Proposition 2.24; we will show that S is also a resolving set.

Now, G has three orbits on pairs of edges (e_1, e_2): where $e_1 = e_2$ (the diagonal orbital), where e_1 is incident with e_2, and where e_1 is not incident with e_2. Label these orbitals as 0, 1 and 2 respectively. Also, label the edges of S as $\{x_1,\ldots,x_t\}$ (where $t = \frac{2}{3}n$), so that incident pairs of edges are labelled x_{2i-1}, x_{2i}. Choose an arbitrary $e \in E(K_n)$. There are five possibilities for $\mathcal{O}(e|S)$:

1. If $e = x_i \in S$, then $\mathcal{O}(x_i|S)$ contains a 0 in position i, with another entry of 1 and all other entries 2.
2. If $\{e, x_{2i-1}, x_{2i}\}$ forms a triangle in K_n, then $\mathcal{O}(x_i|S) = (2,\ldots,2,1,1,2,\ldots,2)$ (where the 1s are in entries $2i-1$ and $2i$).

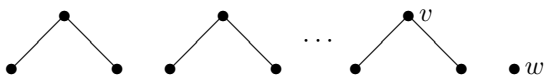
In the remaining cases, e is an edge joining two incident pairs of edges in S, as indicated in the figure below:



3. If $e = uw$, $\mathcal{O}(e|S) = (2,\ldots,2,1,1,2,\ldots,2,1,1,2,\ldots,2)$ (where the 1s are in entries $2i-1$, $2i$, $2j-1$ and $2j$).
4. If $e = uz$, $\mathcal{O}(e|S) = (2,\ldots,2,1,1,2,\ldots,2,1,2,2,\ldots,2)$ (where the 1s are in entries $2i-1$, $2i$ and $2j-1$).
5. If $e = vz$, $\mathcal{O}(e|S) = (2,\ldots,2,1,2,\ldots,2,1,2,\ldots,2)$ (where the 1s are in entries $2i$ and $2j-1$).

We observe that the same sequence can never appear more than once in any of the five cases. Hence S is a resolving set for G. Since we know that S is a base for G of least possible size, it follows that it must also be a resolving set of least possible size, and so $b(G) = \mu(G) = \frac{2}{3}n$.

When $n \equiv 1 \pmod 3$, a similar argument can be used. Now, a minimal base for G in this case is as shown below:



However, this is not a resolving set G; the edge vw cannot be distinguished from the edge forming a triangle with the edges incident with v. However, by adding the edge vw, the set $S \cup \{vw\}$ *is* a resolving set for G. Thus $\mu(G) = b(G) + 1 = \frac{2}{3}(n-1) + 1$.

When $n \equiv 2 \pmod 3$, the same difficulty arises. The following is a minimal base for G:

Again, we can add the extra edge vw to S to obtain a resolving set, which has size $b(G) + 1 = \frac{2}{3}(n-2) + 2$.

The requirement that $n \geq 6$ follows from the fact that when $n = 5$, the problem case does not arise; in that situation, $b(G) = \mu(G) = 3$. □

As a direct consequence, we obtain the following result on metric dimension.

COROLLARY 3.33. *For $n \geq 6$, the class dimension of the Johnson scheme $J(n,2)$ (and thus the metric dimension of the Johnson graph $J(n,2)$ and Kneser graph $K(n,2)$) is given by $\mu(J(n,2)) = \mu(K(n,2)) = \frac{2}{3}(n-i) + i$, where $n \equiv i \pmod 3$, $i \in \{0,1,2\}$.*

In the cases where $n \leq 5$, we note that $J(3,2)$ is the complete graph K_3 (which has metric dimension 2: recall Proposition 3.5), $J(4,2)$ is the octahedron (which has metric dimension 3: this is a straightforward exercise), and that $K(5,2)$ is the Petersen graph (which has metric dimension 3: recall Example 3.3).

3.9. *Connections with the graph isomorphism problem*

Babai's motivation in proving Proposition 3.29 was the graph isomorphism problem. He has provided us with the following comment:

> In fact, breaking regularity is one of the key tools in the design of algorithms for graph isomorphism; the graph isomorphism problem has therefore been one of the strongest motivators of the study of all sorts of "resolving/discriminating sets", and perhaps the only deep motivator of the study of those in contexts where no group is present. In particular, this was the critical motivation behind Weisfeiler and Leman's paper [**95**], my own work [**4**], and also the work of Evdokimov and Ponomarenko.
>
> For instance if the metric dimension of a graph Γ is m then one can give the graph a canonical labeling in essentially n^m steps (n is the number of vertices) and thereby deciding isomorphism of Γ against any graph in about the same amount of time. (The more precise timing would be $O(n^{m+2})$.) The same is true for "my" dimension of a graph (take the coherent configuration generated by the graph and look at its "class dimension") and the EP-dimension (which is always less than or equal to "my" dimension, as you point out).

The work of Evdokimov and Ponomarenko, and the notion of EP-dimension, referred to in the above will be discussed later, in Section 5.

4. *The dimension jump*

One question regarding base size and metric dimension that has arisen repeatedly (albeit under different names) stems from the inequality $b(G) \leq \mu(G)$ (or that $b(\mathrm{Aut}(\Gamma)) \leq \mu(\Gamma)$): namely, how large can the gap between the two parameters be? More specifically, can the gap between the two parameters be made arbitrarily large? This question is asked by Boutin [**19**] and (implicitly) by Vince [**93**], while the paper by Cáceres *et al.* [**28**] is devoted to investigating it. In the same vein, we can ask: for which graphs the two parameters are equal? To aid discussing these questions, we make the following definition.

DEFINITION 4.1. The *dimension jump* of a permutation group G is $\delta(G) = \mu(G) - b(G)$. The *dimension jump* of a graph Γ is defined to be $\delta(\Gamma) = \mu(\Gamma) - b(\mathrm{Aut}(\Gamma))$.

Clearly, if $G = S_n$ in its natural action, $\delta(G) = 0$, since both $b(S_n)$ and $\mu(S_n)$ are equal to $n - 1$. Likewise, $\delta(K_n) = 0$. The next example shows a more interesting infinite family where the dimension jump is also 0.

EXAMPLE 4.2. As we observed in Theorem 3.32, in the case where $n \equiv 0 \pmod 3$, the Johnson graph $\Gamma = J(n, 2)$ (and its complement, the Kneser graph $K(n, 2)$) satisfy $\mu(\Gamma) = b(\mathrm{Aut}(\Gamma)) = \frac{2}{3}n$. Thus we have $\delta(\Gamma) = 0$.

Theorem 3.32 also shows that the Johnson graphs $J(n, 2)$ when $n \not\equiv 0 \pmod 3$ are an infinite family where the dimension jump is constant but non-zero, as in this case we have $\delta(J(n, 2)) = 1$. On the other hand, a number of papers have found examples of families of graphs for which $\delta(\Gamma) \to \infty$.

EXAMPLE 4.3. Fijavž and Mohar [**55**] considered the Paley graphs P_p where p is prime (recall subsection 3.7). In this situation, the base size of $\mathrm{Aut}(P_p)$ is 2, since this group is a Frobenius group (recall Example 2.29). The lower bound in Theorem 3.28 shows that $\mu(P_p) \geq \lfloor \log_2 p \rfloor$; thus it follows that by choosing a sufficient large prime, $\delta(P_p)$ can be made arbitrarily large.

EXAMPLE 4.4. In earlier sections, we have discussed the hypercube $H(d, 2)$ and its automorphism group $G = \mathrm{Aut}(H(d, 2)) = S_2 \wr S_d$. Boutin [**20**] showed that $b(G) = \lceil \log_2 d \rceil + 1$ (see subsection 2.4), while Sebő and Tannier [**85**] observed that Lindström's work [**79**] shows that $\mu(H(d, 2)) = \frac{2d}{\log_2 d}(1 + o(1))$ (see Theorem 3.23). Thus for the dimension jump, we have

$$\delta(G) = \delta(H(d, 2)) = \Theta\left(\frac{2d}{\log_2 d}\right),$$

which can be made arbitrarily large.

Cáceres *et al.* [**28**] considered both the metric dimension of the square lattice graphs $H(2, n)$ and the base size of its automorphism group $S_n \wr S_2$ (see subsections 2.4 and 3.6), obtaining exact values in each case. This gives the following.

EXAMPLE 4.5. From Example 2.16, we have $b(\mathrm{Aut}(H(2, n))) = b(S_n \wr S_2) = n$, while from Theorem 3.25 we have $\mu(H(2, n)) = \lfloor \frac{2}{3}(2n - 1) \rfloor$. Thus $\delta(H(2, n)) = \lfloor \frac{2}{3}(\frac{1}{2}n - 1) \rfloor$, which can be made arbitrarily large.

If a graph has trivial automorphism group, then the base size of its automorphism group is 0. Consequently, the following example gives graphs with arbitrarily large dimension jump (albeit examples which are not so interesting from the group-theoretical perspective).

EXAMPLE 4.6. Cáceres *et al.* [**28**] construct an infinite family of trees T_n by attaching n paths, of lengths $1, 2, \ldots, n$, to a distinguished root vertex. For $n \geq 3$, T_n has trivial

automorphism group, so $b(\mathrm{Aut}(T_n)) = 0$. However, the metric dimension of T_n is $n-1$: a resolving set consists of the end vertices of $n-1$ of the n paths. Thus $\delta(T_n) \to \infty$.

In fact, having $\delta(\Gamma)$ arbitrarily large is a property of "most" graphs in a meaningful way, as the next example shows.

EXAMPLE 4.7. Consider a random graph $G(n,p)$ (see Chapter VII of Bollobás [**17**] for background); all results we mention hold asymptotically almost surely. Now, the diameter of a random graph is 2 (see Bollobás [**17**], Section VII.2), so Proposition 3.6 gives a lower bound on $\mu(G(n,p))$ of approximately $\log_2 n$. Also, in 1963 Erdős and Rényi [**46**] showed that the automorphism group of $G(n,p)$ is trivial, so has base size 0. Thus $\delta(G(n,p)) \to \infty$.

Babai *et al.* [**6**] showed that, in a random graph in $G(n, \frac{1}{2})$, the set of $3\log n$ vertices of highest degree all have different degrees, and form a resolving set (asymptotically almost surely). This results in a canonical labelling of almost all graphs in time linear in the number of edges.

5. *Other directions*

5.1. *Bases for coherent configurations*

Related to their work with Karpinski on the graph isomorphism problem (see [**48**]), in [**49**, **51**] Evdokimov and Ponomarenko introduced the notion of a *base* for a coherent configuration. (We shall refer to these as *EP-bases*.) A remark in [**50**] suggests that a resolving set in Babai's sense (see Definition 3.13) is necessarily a base in their sense (and thus that the size of an EP-base is bounded by the class dimension), though no proof is offered. In this subsection we consider these two notions and prove the assertion, and also observe that the converse is false. We will see that the gap between the two parameters can be arbitrarily large.

First, a comment about coherent configurations. Let $\mathcal{X}$ be any set of binary relations on a finite set Ω. Then there is a unique coherent configuration $\mathcal{C}$ on Ω which is coarsest with respect to being a refinement of $\mathcal{X}$. This is most easily explained in terms of the corresponding cellular algebra. Slightly more generally, let $\mathcal{A}$ be any set of $\Omega \times \Omega$ matrices, containing the identity matrix. Close $\mathcal{A}$ under addition, scalar multiplication, matrix multiplication, and the following: if $A \in \mathcal{A}$ and c is some entry of A, then the zero-one matrix with 1 in the positions where A has entry c and 0 elsewhere is in A. The resulting set of matrices is the cellular algebra of a coherent configuration, which we call the *coherent configuration generated by* $\mathcal{A}$.

Suppose that a set $\mathcal{X}$ of relations is given. Define an equivalence relation on $\Omega \times \Omega$ by the rule that (x,y) and (u,v) are equivalent if and only if, for any word in the elements of $\mathcal{X}$, the number of (x,y) paths with edges described by the entries in the word is equal to the number of such (u,v) paths. The resulting partition of $\Omega \times \Omega$ is coarser than the coherent configuration generated by $\mathcal{X}$. (If we iterate this procedure until it stabilises, we obtain the coherent configuration generated by $\mathcal{X}$.)

Now we turn to the definition of an EP-base.

DEFINITION 5.1. Let $\mathcal{R} = \{R_1, \ldots, R_r\}$ be a coherent configuration on Ω, and $(v_1, \ldots, v_b)$ be a sequence of points from Ω. We say that $(v_1, \ldots, v_b)$ is an *EP-base* if the coherent configuration generated by $\mathcal{R} \cup \{I_{v_1}, \ldots, I_{v_b}\}$ is trivial, in that all classes are singletons (where I_v is the relation $\{(v,v)\}$). We call the size of the smallest EP-base the *EP-dimension* of the configuration.

In the case where $\mathcal{R}$ arises from a group G, both a resolving set and an EP-base are bases for G, so both "dimensions" are upper bounds for the base size of G.

PROPOSITION 5.2. *If a sequence in a coherent configuration is a resolving set, then it is an EP-base. Hence the EP-dimension of a coherent configuration does not exceed its class dimension.*

Proof. Let $\mathcal{R}$ be a coherent configuration, and suppose $S = (v_1, \ldots, v_b)$ is a resolving set for it. Given any distinct points x and y, their "codes" $\mathcal{O}(x|S)$ and $\mathcal{O}(y|S)$ differ, so there is a point $v_i \in S$ such that the relations $C(x, v_i)$ and $C(y, v_i)$ differ. Now, thinking of $\mathcal{R}$ as a colouring of the arcs of a complete directed graph, then if $R = C(x, v_i)$, there is one (R, I_{v_i}, R^*) path from x to x, and none from y to y. So (x, x) and (y, y) lie in different relations in the configuration generated by $\mathcal{R}$ and $I_{v_1}, \ldots, I_{v_b}$. Again since x and y are arbitrary, this shows that $(v_1, \ldots, v_b)$ is an EP-base. □

The converse of the proposition is false: Theorem 1.2 of Evdokimov and Ponomarenko's 2002 paper [**52**] implies that the EP-dimension of the Paley graph P_p is 2 for all $p \equiv 1 \mod 4$. On the other hand, Theorem 3.28 shows that the class dimension $c = \Omega(\log_2 p)$. Consequently, this shows that the gap between the two parameters can be arbitrarily large.

There are other cases where the two parameters agree. The group S_n on 2-sets, where n is a multiple of 3, has the base size of the group and the class dimension of the corresponding coherent configuration both equal to $2n/3$ (see Theorem 3.32); the EP-dimension is sandwiched between, and so is also $2n/3$.

5.2. *Robinson's bound*

In Section 2, we saw how results on base sizes from the graph theory literature can be generalised to a more algebraic setting. Not surprisingly, there are also results from the group theory literature which can be reinterpreted graph-theoretically. In this subsection, we describe such a result.

In [**83**], Robinson obtained the following bound on the base size of a primitive permutation group in terms of its degree and rank.

THEOREM 5.3 (Robinson [**83**]). *Suppose G is a primitive permutation group of degree n and rank r. Then*

$$b(G) \leq \frac{n-1}{r-1}.$$

There are two proofs in the literature, which are both algebraic in nature. Robinson's original proof uses character theory, while Evdokimov and Ponomarenko [**49**, **51**] obtained the result as a corollary to a corresponding one for EP-bases (as defined above). However, in the case where G is the automorphism group of a primitive distance-transitive graph Γ, then we can easily rephrase Robinson's bound graph-theoretically.

COROLLARY 5.4. *Suppose Γ is a primitive distance-transitive graph with n vertices and diameter d. Then*

$$b(\mathrm{Aut}(\Gamma)) \leq \frac{n-1}{d}.$$

The hypothesis cannot be weakened to imprimitive distance-transitive graphs: for the complete bipartite graph $K_{m,m}$, we have $n = 2m$ and $d = 2$, but $b(\mathrm{Aut}(K_{m,m})) = 2m - 2$ which exceeds the bound. However, it would be interesting to see where this result holds for other classes of graphs.

5.3. *Extensions of orbital dimension*

As we saw in Corollary 3.18, a group G of degree n has orbital dimension $n - 1$ if and only if G is 2-transitive. There are even examples of 2-transitive groups where the gap between base size and orbital dimension is as large as possible.

EXAMPLE 5.5. Suppose G is sharply 2-transitive. Zassenhaus showed that a sharply 2-transitive group of degree n exists if and only if n is a prime power (see Dixon and Mortimer [**44**], Section 7.6). By Corollary 3.18, $\mu(G) = n - 1$; however, it follows from the definition that $b(G) = 2$.

Consequently, orbital dimension does not convey much information about 2-transitive groups. However, we can generalise it in the following manner.

The *k-orbits* of G are its orbits on Ω^k, i.e. on k-tuples. So, for instance, the 2-orbits are the orbitals. Suppose G has k-orbits $C_1, \ldots, C_r$. For a given $(k-1)$-tuple $T = (t_1, \ldots, t_{k-1})$, we let $\mathcal{C}(T, y)$ denote the unique k-orbit containing $(t_1, \ldots, t_{k-1}, y)$. Then for a subset $S \subseteq \Omega$, we define a function

$$\mathcal{O}_{k-1}(y|S) \ : \ S^{k-1} \to \{C_1, \ldots, C_r\}$$

where each $(k-1)$-tuple $T \in S^{k-1}$ is mapped to $\mathcal{C}(T, y)$.

DEFINITION 5.6. A subset $S \subseteq \Omega$ is a *k-resolving set* for G if, for any $y \in \Omega$, the value of the function $\mathcal{O}_{k-1}(y|S)$ uniquely identifies y. The *k-orbital dimension* of G is the smallest cardinality of a k-resolving set for G, and is denoted $\mu_k(G)$.

We note that as before, the k-orbital dimension of G gives an upper bound on the base size of G.

EXAMPLE 5.7. If G is sharply 2-transitive, its base size is 2, but so is its 3-orbital dimension. This compares to its 2-orbital dimension of $n - 1$.

EXAMPLE 5.8. Consider the group $G = \mathrm{PSL}(2, p)$, acting on the projective line $\mathbb{F}_p \cup \{\infty\}$. This is an IBIS group where $b(G) = 3$, and there are just two orbits on triples with all entries distinct. Now, we can argue in the same way as Proposition 3.6 that, if $\mu_3(G) = d$, then $d + 2^d \geq p + 1$, so there is a lower bound of about $\log_2 p$ for $\mu_3(G)$. On the other hand, if we take the point ∞ together with a resolving set for the Paley graph P_p, then we have a 3-resolving set for the whole group (indeed taking triples containing ∞ is enough to show this), so there is an upper bound of about $2 \log_2 p$ for $\mu_3(G)$.

5.4. *Infinite structures*

So far, we have only been concerned with finite structures. However, many of the parameters we have discussed (base size, distinguishing number, metric dimension) can be defined for

infinite structures in a meaningful way, and there are examples in the literature where these have been studied. The distinguishing number has perhaps attracted the most interest, and we describe some of the results below.

In their 2007 paper [**67**], Imrich *et al.* considered the countable random graph R (also known as the Rado graph: see [**33**], Section 5.1), which has a large automorphism group, and proved that $\mathrm{Aut}(R)$ has distinguishing number 2. Their result has been generalised in a recent paper of Laflamme *et al.* [**74**], where they considered a broader class of structures. They show that, for many classical examples of countable homogeneous relational structures, their automorphism groups have distinguishing number either 2 or ∞: their examples include countable homogenous graphs (both directed and undirected), the universal poset, and the countable dense linear order $(\mathbb{Q}, \leq)$. Moreover, they show that any countable homogeneous structure satisfying the *free amalgamation property* (see [**33**], Section 5.6) has distinguishing number 2. More recently, Bonato and Delić [**18**] have obtained a further generalisation: they showed that any countable relational structure satisfying a particular adjacency property (which they call the *weak-e.c. property*) has distinguishing number 2.

The metric dimension of infinite graphs has been conisdered by Cáceres *et al.* [**29**]. Naturally, depending on the structure of the graph, metric dimension may be finite or infinite. Among the examples they consider are Cartesian products of infinite graphs, such as the Cartesian product of a (finite) complete graph with a two-way infinite path.

6. *Some open questions*

There are various interesting open questions which arise from the material we have dicussed. We will conclude the paper by mentioning some of these.

IBIS graphs

In subsection 2.6, we considered graphs for which the automorphism group is an IBIS group (i.e. the minimal bases have the same size). Examples include complete graphs, vertex-transitive graphs of prime order (see Proposition 2.28), and a class of outerplanar graphs characterised by Boutin [**21**].

Problem. Find further examples of IBIS graphs (i.e. graphs whose automorphism group is an IBIS group).

It would be particularly interesting to find families of IBIS graphs which have a strong symmetry or regularity property. We note, however, that it fails for Johnson and Kneser graphs.

Resolving sets and the exchange property

In [**21**], as well as considering IBIS graphs, Boutin also asks when minimal resolving sets satisfy the exchange property (and so form the bases of a matroid). Clearly, complete graphs have this property; Boutin also shows that it holds for trees.

Problem. Find further examples of graphs whose minimal resolving sets satisfy the exchange property.

As with IBIS graphs, it would be interesting to find examples with a strong symmetry or regularity property.

Complexity of class dimension and orbital dimension

In subsection 3.1, we saw that the problem of determining the metric dimension of a graph is NP-hard. It therefore seems natural to ask the same question for the class dimension of a coherent configuration.

PROBLEM. What is the computational complexity of determing the class dimension of a coherent configuration?

We anticipate that this problem is also likely to be NP-hard.

Bounds on class dimension

In subsection 3.1, Theorem 3.7 (due to Hernando *et al.*) gave an upper bound on the number of vertices of a graph with given metric dimension and diameter. This is an improvement of Proposition 3.6, which also holds for the class dimension of coherent configurations (Proposition 3.19). So one could ask for an analogue of the result of Hernando *et al.*

PROBLEM. Find an upper bound on the number of points in a coherent configuration of given class dimension and rank, which is an analogy of Theorem 3.7.

We remark that the proof used by Hernando *et al.* [**63**] does not carry over to coherent configurations directly, as it uses the fact that graph distance satisfies the triangle inequality, which we don't have for general coherent configurations. (In fact, it holds precisely for distance-regular graphs, where we already have the bound for metric dimension.)

Metric dimension of graphs with classical parameters

In subsections 3.6 and 3.8, we considered the metric dimension of certain Hamming and Johnson graphs. These are just two of the well-known families of *graphs with classical parameters*, described in Chapter 9 of Brouwer, Cohen and Neumaier [**22**]. As these graphs are all distance-regular, then as we have seen this is equivalent to finding the class dimension of the corresponding association schemes.

PROBLEM. Find the class dimension of the Johnson scheme $J(n, k)$, for $k > 2$.

This task may be helped by the existing results on the base size of its automorphism group (S_n in its action on k-subsets), such those of Maund (Theorem 2.22) and Cáceres *et al.* (Theorem 2.25).

PROBLEM. Find the metric dimension of Grassmann graphs, dual polar graphs, and graphs arising from sesquilinear or quadratic forms (see [**22**], Chapter 9 for definitions of these).

Work is in progress on both of these problems [**9**, **10**].

Acknowledgements. The authors would especially like to thank Professor L. Babai for numerous helpful comments and suggestions which helped improve the paper. The first author is a PIMS Postdoctoral Fellow, and also wishes to thank NSERC and the Ontario Ministry of Research and Innovation for their financial support.

References

1. M. O. Albertson and D. L. Boutin, 'Using determining sets to distinguish Kneser graphs', *Electron. J. Combin.* 14(1) (2007), #R20.
2. M. O. Albertson and K. L. Collins, 'Symmetry breaking in graphs', *Electron. J. Combin.* 3(1) (1996), #R18.
3. L. Babai 'Asymmetric trees with two prescribed degrees', *Acta Math. Acad. Sci. Hungar.* 29 (1977), 193–299.
4. L. Babai, 'On the complexity of canonical labeling of strongly regular graphs', *SIAM J. Comput.* 9 (1980), 212–216.
5. L. Babai, 'On the order of uniprimitive permutation groups', *Ann. Math.* 113 (1981), 553–568.
6. L. Babai, P. Erdős and S. M. Selkow, 'Random graph isomorphism', *SIAM J. Comput.* 9 (1980), 628–635.
7. R. A. Bailey, *Association Schemes: Designed Experiments, Algebra and Combinatorics* (Cambridge University Press, Cambridge, 2004).
8. R. F. Bailey, 'Uncoverings-by-bases for base-transitive permutation groups', *Des. Codes Cryptogr.* 41 (2006), 153–176.
9. R. F. Bailey, J. Cáceres, D. Garijo, A. Gonzales, A. Márquez, K. Meagher and M. L. Puertas, 'Resolving sets in Johnson and Kneser graphs', in preparation.
10. R. F. Bailey and K. Meagher, 'On the metric dimension of Grassmann graphs', preprint.
11. E. Bannai, R. L. Griess, C. E. Praeger and L. L. Scott, 'The mathematics of Donald Gordon Higman', *Michigan Math. J.* 58 (2009), 3–30.
12. E. Bannai and T. Ito, *Algebraic Combinatorics. I: Association Schemes* (Benjamin/Cummings, Menlo Park, 1984).
13. C. Benbenishty, 'On actions of primitive groups', Ph.D. thesis, Hebrew University of Jerusalem, 2005.
14. N. L. Biggs, *Algebraic Graph Theory*, 2nd Edition (Cambridge University Press, Cambridge, 1993).
15. K. D. Blaha, 'Minimum bases for permutation groups: the greedy approximation', *J. Algorithms* 13 (1992), 297–306.
16. A. Bochert, 'Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann', *Math. Ann.* 33 (1889), 584–590.
17. B. Bollobás, *Modern Graph Theory*, Graduate Texts in Mathematics 184 (Springer–Verlag, New York, 1998).
18. A. Bonato and D. Delić, 'Distinguishing number and adjacency properties', *J. Combinatorics* 6 (2010), 1–2.
19. D. L. Boutin, 'Identifying graph automorphisms using determining sets', *Electron. J. Combin.* 13(1) (2006), #R78.
20. D. L. Boutin, 'The determining number of a Cartesian product', *J. Graph Theory* 61 (2009), 77–87.
21. D. L. Boutin, 'Determining sets, resolving sets, and the exchange property', *Graphs Combin.* 25 (2009), 789–806.
22. A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs* (Springer–Verlag, Berlin, 1989).
23. T. C. Burness, 'On base sizes for actions of finite classical groups', *J. London Math. Soc. (2)* 75 (2007), 545–562.
24. T. C. Burness, R. M. Guralnick and J. Saxl, 'Base sizes for actions of simple groups', in preparation.
25. T. C. Burness, M. W. Liebeck and A. Shalev, 'Base sizes for simple groups and a conjecture of Cameron', *Proc. London Math. Soc. (3)* 98 (2009), 116–162.
26. T. C. Burness, E. A. O'Brien and R. A. Wilson, 'Base sizes for sporadic groups', *Israel J. Math.*, 177 (2010), 307–334.
27. J. Cáceres, D. Garijo, A. Gonzales, A. Márquez and M. L. Puertas, 'Hypergraphs for computing determining sets of Kneser graphs', preprint.
28. J. Cáceres, D. Garijo, M. L. Puertas and C. Seara, 'On determining number and metric dimension of graphs', *Electron. J. Combin.* 17(1) (2010), #R63.
29. J. Cáceres, C. Hernando, M. Mora, I. M. Pelayo and M. L. Puertas, 'On the metric dimension of infinite graphs', preprint; `arxiv.org/abs/0904.4826`.
30. J. Cáceres, C. Hernando, M. Mora, I. M. Pelayo, M. L. Puertas, C. Seara and D. R. Wood, 'On the metric dimension of Cartesian products of graphs', *SIAM J. Discrete Math.* 21 (2007), 423–441.
31. P. J. Cameron, 'Regular orbits of permutation groups on the power set', *Discrete Math.* 62 (1986), 307–309.
32. P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms* (Cambridge University Press, Cambridge, 1994).
33. P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts 45 (Cambridge University Press, Cambridge, 1999).
34. P. J. Cameron, 'Coherent configurations, association schemes and permutation groups', *Groups, Combinatorics and Geometry* (eds A. A. Ivanov, M. W. Liebeck and J. Saxl, World Scientific, Singapore, 2003).
35. P. J. Cameron and D. G. Fon-Der-Flaass, 'Bases for permutation groups and matroids', *Europ. J. Combinatorics* 16 (1995), 537–544.

36. P. J. Cameron and W. M. Kantor, 'Random permutations: some group-theoretic aspects', *Combin. Probab. Comput.* 2 (1993), 257–262.

37. P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Mathematical Society Student Texts 22 (Cambridge University Press, Cambridge, 1991).

38. P. J. Cameron, P. M. Neumann and J. Saxl, 'On groups with no regular orbits on the set of subsets', *Arch. Math. (Basel)* 43 (1984), 295–296.

39. G. Chartrand, L. Eroh, M. A. Johnson and O. R. Oellermann, 'Resolvability in graphs and the metric dimension of a graph', *Discrete Appl. Math.* 105 (2000), 99–113.

40. V. Chvátal, 'Mastermind', *Combinatorica* 3 (1983), 325–329.

41. K. L. Collins and A. N. Trenk, 'The distinguishing chromatic number', *Electron. J. Combin.* 13(1) (2006), #R16.

42. J. D. Currie and O. R. Oellermann, 'The metric dimension and metric independence of a graph', *J. Combin. Math. Combin. Comput.* 39 (2001), 157–167.

43. D. Cvetković, M. Čangalović, V. Kovačević-Vujčić and J. Kratica, 'Distance-perfect graphs', *Proceedings of SYM–OP–IS 2007 (Zlatibor, Serbia)*, 2007.

44. J. D. Dixon and B. C. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163 (Springer–Verlag, New York, 1996).

45. S. Dolfi, 'Orbits of permutation groups on the power set', *Arch. Math. (Basel)* 75 (2000), 321–327.

46. P. Erdős and A. Rényi, 'Asymmetric graphs', *Acta Math. Acad. Sci. Hungar.* 14 (1963), 295–315.

47. P. Erdős and A. Rényi, 'On two problems of information theory', *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, 8 (1963), 229–243.

48. S. A. Evdokimov, M. Karpinski and I. N. Ponomarenko, 'On a new high-dimensional Weisfeiler–Lehman algorithm', *J. Algebraic Combin.* 10 (1999), 29–45.

49. S. A. Evdokimov and I. N. Ponomarenko, 'On primitive cellular algebras', *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* 256 (1999), 38–68 (in Russian).

50. S. A. Evdokimov and I. N. Ponomarenko, 'Separability number and Schurity number of coherent configurations', *Electron. J. Combin.* 7 (2000), #R31.

51. S. A. Evdokimov and I. N. Ponomarenko, 'On primitive cellular algebras', *J. Math. Sci. (New York)* 107 (2001), 4172–4191 (English translation of [**49**]).

52. S. A. Evdokimov and I. N. Ponomarenko, 'Characterization of cyclotomic schemes and normal Schur rings over a cyclic group', *Algebra i Analiz* 14 (2002), 11–55 (in Russian); English translation: *St Petersburg Math. J.* 14 (2003), 189–221.

53. D. Erwin and F. Harary, 'Destroying automorphisms by fixing nodes', *Discrete Math.* 306 (2006), 3244–3252.

54. I. A. Faradžev, A. A. Ivanov, M. H. Klin and A. J. Woldar (eds), *Investigations in algebraic theory of combinatorial objects*, Mathematics and its Applications (Soviet Series) 84 (Kluwer, Dordrecht, 1994).

55. G. Fijavž and B. Mohar, 'Rigidity and separation indices of Paley graphs', *Discrete Math.* 289 (2004), 157–161.

56. G. Fijavž and B. Mohar, 'Rigidity and separation indices of graphs in surfaces', preprint.

57. M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (W. H. Freeman, San Francisco, 1979).

58. C. R. Gibbons and J. D. Laison, 'Fixing numbers of graphs and groups', *Electron. J. Combin.* 16(1) (2009), #R39.

59. D. Gluck and K. Magaard, 'Base sizes and regular orbits for coprime affine permutation groups', *J. London Math. Soc. (2)* 58 (1998), 603–618.

60. D. Gluck, Á. Seress and A. Shalev, 'Bases for primitive permutation groups and a conjecture of Babai', *J. Algebra* 199 (1998), 367–378.

61. J. J. Graham and G. I. Lehrer, 'Cellular algebras', *Invent. Math.* 123 (1996), 1–34.

62. F. Harary and R. A. Melter, 'On the metric dimension of a graph', *Ars Combin.* 2 (1976), 191–195; 4 (1977), 318.

63. C. Hernando, M. Mora, I. M. Pelayo, C. Seara and D. R. Wood, 'Extremal graph theory for metric dimension and diameter', *Electron. J. Combin.* 17(1) (2010), #R30.

64. D. G. Higman, 'Coherent configurations. I', *Rend. Sem. Mat. Univ. Padova* 44 (1970), 1–25.

65. W. Imrich and S. Klavžar, *Product Graphs: Structure and Recognition* (Wiley-Interscience, New York, 2000).

66. W. Imrich and S. Klavžar, 'Distinguishing Cartesian powers of graphs', *J. Graph Theory* 53 (2006), 250–260.

67. W. Imrich, S. Klavžar and V. I. Trofimov, 'Distinguishing infinite graphs', *Electron. J. Combin.* 14(1) (2007), #R36.

68. J. P. James, 'Two point stabilisers of partition actions of linear groups', *J. Algebra* 297 (2006), 453–469.

69. J. P. James, 'Partition actions of symmetric groups and regular bipartite graphs', *Bull. London Math. Soc.* 38 (2006), 224–232.

70. G. Kabatianski, V. Lebedev and J. Thorpe, 'The Mastermind game and the rigidity of the Hamming space', *Proceedings of IEEE International Symposium on Information Theory (Sorrento, Italy)*, 2000.

71. S. Khuller, B. Raghavachari and A. Rosenfeld, 'Landmarks in graphs', *Discrete Appl. Math.* 70 (1996), 217–229.

72. J. Kratica, D. Cvetković, M. Čangalović, V. Kovačević-Vujčić and J. Kojić, 'The metric dimension of strongly regular graphs', *Proceedings of SYM–OP–IS 2008 (Belgrade)*, 2008.
73. J. Kratica, V. Kovačević-Vujčić and M. Čangalović, 'Computing the metric dimension of graphs by genetic algorithms', *Comput. Optim. Appl.* 44 (2009), 343–361.
74. C. Laflamme, L. Nguyen Van Thé and N. W. Sauer, 'Distinguishing number of countable homogeneous relational structures', *Electron. J. Combin.* 17(1) (2010), #R20.
75. M. W. Liebeck and A. Shalev, 'Simple groups, permutation groups, and probability', *J. Amer. Math. Soc.* 12 (1999), 497–520.
76. M. W. Liebeck and A. Shalev, 'Bases of primitive linear groups', *J. Algebra* 252 (2002), 95–113.
77. M. W. Liebeck and A. Shalev, 'Bases of primitive permutation groups', *Groups, Combinatorics and Geometry* (eds A. A. Ivanov, M. W. Liebeck and J. Saxl, World Scientific, Singapore, 2003), 147–154.
78. M. W. Liebeck and A. Shalev, 'Character degrees and random walks in finite groups of Lie type', *Proc. London Math. Soc. (3)* 90 (2005), 61–86.
79. B. Lindström, 'On a combinatory detection problem. I', *Magyar Tud. Akad. Mat. Kutató Int. Közl.* 9 (1964), 195–207.
80. T. Maund, 'Bases for permutation groups', D.Phil. thesis, University of Oxford, 1989.
81. J. G. Oxley, *Matroid Theory* (Oxford University Press, Oxford, 1992).
82. L. Pyber, 'Asymptotic results for permutation groups', *Groups and Computation* (eds L. Finkelstein and W. M. Kantor), DIMACS Series on Discrete Math. and Theor. Computer Science 11 (American Mathematical Society, Providence, 1993), 197–219.
83. G. R. Robinson, 'On the base size and rank of a primitive permutation group', *J. Algebra* 187 (1997), 320–321.
84. G. Sabidussi, 'Graph multiplication', *Math. Z.* 72 (1960), 446–457.
85. A. Sebő and E. Tannier, 'On metric generators of graphs', *Math. Oper. Res.* 29 (2004), 383–393.
86. Á. Seress, 'The minimal base size of primitive solvable permutation groups', *J. London Math. Soc. (2)* 53 (1996), 243–255.
87. Á. Seress, 'Primitive groups with no regular orbits on the set of subsets', *Bull. London Math. Soc.* 29 (1997), 697–704.
88. Á. Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics 152 (Cambridge University Press, Cambridge, 2003).
89. C. C. Sims, 'Determining the conjugacy classes of a permutation group', *Computers in Algebra and Number Theory* (eds G. Birkhoff and M. Hall, Jr., American Mathematical Society, Providence, 1971), 191–195.
90. P. J. Slater, 'Leaves of trees', *Congr. Numer.* 14 (1975), 549–559.
91. D. H. Smith, 'Primitive and imprimitive graphs', *Quart. J. Math. Oxford Ser. (2)* 22 (1971), 551–557.
92. E. Spence, 'Strongly regular graphs on at most 64 vertices', `http://www.maths.gla.ac.uk/~es/srgraphs.html`.
93. A. Vince, 'Separation index of a graph', *J. Graph Theory* 41 (2002), 53–61.
94. V. G. Vizing, 'The Cartesian product of graphs', *Vyčisl. Sistemy* 9 (1963), 30–43 (in Russian).
95. B. Yu. Weisfeiler and A. A. Leman, 'Reduction of a graph to a canonical form and an algebra which appears in this process', *Scientific-Technological Investigations Ser. 2*, 9 (1968), 12–16 (in Russian).
96. P.-H. Zieschang, *Theory of Association Schemes* (Springer–Verlag, Berlin, 2005).
97. B. Zil'ber, 'Finite homogeneous geometries', *Seminarber., Humboldt-Univ. Berlin, Sekt. Math.* 98 (1988), 186–208.

Robert F. Bailey
Department of Mathematics and Statistics
University of Regina
3737 Wascana Parkway
Regina, Saskatchewan S4S 0A2
Canada

robert.bailey@uregina.ca

Peter J. Cameron
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road
London E1 4NS

p.j.cameron@qmul.ac.uk